Proceedings of the World Congress on Engineering 2007 Vol II
WCE 2007, July 2 - 4, 2007, London, U.K.

A Brief Survey on RFID Privacy and Security

J. Aragones-Vilella*, A. Martínez-Ballesté and A. Solanas
CRISES Reserch Group
UNESCO Chair in Data Privacy
Dept. of Computer Engineering and Mathematics,
Rovira i Virgili University
Av. Països Catalans 26, E-43007 Tarragona, Catalonia, Spain
e-mail {jordi.aragones,antoni.martinez,agusti.solanas}@urv.cat

Abstract— **In this survey we take a look at different approaches proposed in the literature for addressing the privacy and security issues derived from the Radio-Frequency IDentification (RFID) deployment. We concentrate on the lack of privacy that RFID users can suffer from, and we elaborate on how the security in the communications between RFID devices can be assured. The main goal of this brief survey is giving a concise classification of the most relevant privacy protection protocols applied to RFID technology. For the sake of brevity and clarity, only the most relevant approaches are selected and classified according to the computational power of the utilised passive devices (*i.e.* the tags).**

Keywords: **RFID, privacy, security, authentication**

1 Introduction

Radio-Frequency IDentification (RFID) devices have an important presence in our daily life, even when we do not see them, and they will become ubiquitous in the near future. The spectacular market push of RFID technology is due to the interest by large retailers (*e.g.* Wal-Mart [1]), important manufacturers (*e.g.* Gillette, Procter & Gamble, etc.) and governments. As a result, almost every object is liable to carry an RFID tag. RFID devices can be seen as a proper substitute of bar codes since they are mainly used to identify objects. Unlike bar codes, RFID devices allow objects to be identified without visual contact and help in improving and automating many processes *e.g.* supermarket checkouts, product inventories, etc. This is possible due to the ability of RFID tags for being read fast and in parallel. An RFID system consists of two main components:

- *RFID tags*: They are small passive devices with a variety of possible appearances from stickers to small grains embedded in official documents. A tag basically consists of a microchip and a metal coil, which acts as an antenna. In some cases, it can also contain a battery and some other microchips intended for increasing its computational power.
- *RFID readers*: They are active devices used to read the information stored in the tags. In a nutshell, readers emit a radio wave so that all tags in their range *answer* by broadcasting their embedded information (*i.e.* a set of bits). This information, generally known as *Electronic Product Code* (EPC), is usually the identifier of the object into which the tags are stuck.

It is possible to find in the market UHF-tags which can be read from a distance of up to 10 meters, and HF-tags which can be read from a distance of up to 2 meters. These maximum distances can be shortened by the environment. In [19] those ranges are classified as:

- *Nominal read range:* This is the range indicated by RFID standards and product specifications. It is the maximum distance from which a tag can be read by a reader.
- *Rogue scanning range:* This is the maximum range, out of legal limits, from which a reader can power and read a tag.
- *Tag-to-reader eavesdropping range:* When a reader powers a tag, a more sensitive receiver can eavesdrop the emissions of a tag without emitting any signal. Thus, the eavesdropper range can be equal to or higher than the rogue scanning range.
- *Reader-to-tag eavesdropping range:* This range is even higher than the previous one because the power of the signal of the reader is greater than the one of the tag.
- *Detection range:* This is the range from which tags or readers can be detected. Note that it does not necessary mean to be able to send or receive information. Thus, this range is the highest.

*The authors sign in alphabetical order.

[1] Wal-Mart started to explore the RFID technology in 2003 and devoted at least three billion dollars to implement it [14].

Although a variety of RFID classifications can be found in the literature, we believe that the next one, based on the computational power of the tags, is the most interesting from the privacy and security point of view. We can classify tags in three main categories according to their computational power:

1. *Elemental or basic tags*, which are not capable of performing cryptographic operations such as generating random values or computing hashes.

2. *Symmetric-key tags*, which are capable of dealing with symmetric-key cryptography protocols. They are more expensive than the basic ones.

3. *Public-key tags*, which are capable of managing public-key cryptography protocols. They are the most expensive ones.

This computational-power-based classification will be used as a skeleton for the exposition of the methods in this paper.

A priori, RFID tags can be read by any unauthorised reader in their cover ranges and, for this reason, some security and privacy issues must be taken into account. In fact, an eavesdropper, properly equipped with a reader, could collect lots of information from scanned people *e.g.* the brand of their clothes, the amount of banknotes they have in their pockets, the use of prosthesis or medicines, etc. Moreover, making use of several readers strategically deployed, it could be possible to track the location of tags and, consequently, the motion of the scanned people. Last but not least, an eavesdropper could infer the consumer habits of the scanned people (*e.g.* he could determine whether they frequently visit a certain restaurant or shop).

The aforementioned problems can give cause for concern because a huge deployment of the RFID technology could pave the way for a *big brother effect*. Hence, if no practical solutions are proposed, this huge deployment will not be likely to happen. An example of popular opposition to RFID deployment can be found in 2003, when Benetton was boycotted when they tried to introduce RFID tags in their clothes [2]. In the same year, several private organisations signed an agreement on how to use RFID technology in their products [3]. Moreover, the Directive 2002/58/EC (Directive on privacy and electronic communications [1]) deals with the relationship between Information and Communication Technologies (ICT) and the privacy and security of their users. In addition to classical concepts regarding information security (*e.g.* encryption and digital signatures), the directive elaborates on some issues related to the privacy of ICT users.

Contribution and plan of this paper

In this brief survey we present the main approaches related to RFID security and privacy. The plan of this paper is as follows: Section 2 presents several techniques applied to the basic tags being the aim to achieve certain security and privacy levels. Section 3 summarises some of the main security protocols for symmetric-key tags. Some of the existing proposals based on public-key cryptography for RFID tags are studied in Section 4. Finally, Section 5 concludes the paper.

2 Security in basic tags

Elemental tags are the simplest and cheapest ones of the RFID tags family. These tags are not able to perform cryptographic operations and they are built using from 200 to 2000 gates for security purposes [31]. To guarantee the security and privacy of the owners of these tags several approaches have been proposed.

2.1 Killing and sleeping commands

The `Kill` command is a trustworthy solution for these tags although its use permanently disables the functionality of the tags. The execution of this command is protected by a 32-bit Personal Identification Number (PIN), which will be sent along with the command as a security measure (without the PIN, an attacker could not disable any tag). This technique is equivalent to extract the tag from the product once it has been bought. A different solution consists in using the `Sleep` command for temporarily disabling the tags. People having a tag (*e.g.* carrying it on their brand new jeans) may ask for the execution of the command also using a 32-bit PIN. Unfortunately, these method could pose a problem for people with little expertise in technology.

2.2 The proxying approach

Another possibility for protecting the privacy of an RFID tag is by using a privacy-enforcing device, as a *Watchdog tag* [11] or an *RFID Guardian* [25]. A *Watchdog tag* is a complex tag having a battery, a display and, potentially, a long-range communication channel. The main purpose of this tag is to detect the transmission of readers which are close to it, and to provide the owner with information like the identifier of the reader. An *RFID Guardian* works by searching tags which are close to it, and by managing the access to those tags by means of the authentication of the readers trying to access the tags. If the readers are not authenticated, the *Guardian* blocks the communication. Like the previous approach, this one requires the user to have some technical skills and to own some additional hardware.

2.3 Blocking

This scheme was proposed by Juels, Rivest and Szydlo [21]. It relies on the concept of *blocker tag*. A blocker tag simulates the full spectrum of possible tags. By doing this, it becomes very difficult for a reader to know which tags are really being carried by a given user. The blocker tag can be programmed to generate only a given subset of possible identifiers (*e.g.* the ones of a given manufacturer). This allows the implementation of security zones related to different blocker tags. The main problem of the technique is the existence of malicious blocker tags that can interfere with the proper use of RFID protocols (*e.g.* in a supermarket checkout).

2.4 Tag relabelling

This solution was proposed by Sarma, Weis and Engels [26] in 2002. The main goal of this approach is to avert the possibility of tracking a tag. They suggested to frequently relabel the identifiers of tags and just leave the main information untouched. In this case tags are still usable but their identifiers (*i.e.* the identifier of the product) are lost. Innoue and Yasuura [17] in 2003, proposed to store these identifiers in order to be able to re-activate tags in the future for recycling or reselling them. Good et al. [13] in 2004 gave a particular solution for libraries where tags receive a random number as identifier during the checkout.

2.5 Use of pseudonyms

In [18] Juels suggested the use of a collection of pseudonyms for a given tag with the idea of answering to each query with a different identifier *(i.e.* a pseudonym). An authorised reader stores this collection of identifiers and, thus, it will be able to match the identifier with the tag. On the contrary, a non-authorised reader will only see different identifiers. However, if the same reader polls a tag a sufficient number of times, it will be able to collect the whole list of pseudonyms of a given tag. A possible solution to this attack consists in providing the tag with the ability of detecting the reader that is making the queries and refusing to answer when these queries are too much frequent.

2.6 Re-encryption

The re-encryption proposal of Juels and Pappu [20] could be mainly applied to RFID-enabled banknotes. This scheme uses a public-key cryptosystem with a single key pair (P_K, S_K), where S_K is held by a law enforcement agency. The tag stores a unique identifier and the banknote serial number S. This value is encrypted using P_K, and this cipher text is actually the information answered by the tag. Note that the tag does not perform the encryption, it only answers the cipher text that has been previously stored into it. Only the law enforcement agency can decrypt the cipher text and obtain the serial number. Avoine explores the limitation of this protocol in [4]. The *Universal Re-encryption* is another re-encryption based protocol that permits re-encryption of a cipher text without the knowledge of the corresponding public key [12].

3 Security in symmetric-key RFIDs

In this section we describe the most significant symmetric-key protocols for RFID security and privacy.

3.1 The OSK protocol

This protocol was proposed by Ohkubo, Suzuki and Kinoshita (OSK) in 2004 [23]. Its aim is to assure the valid answer of the tag even under an active attack. In this scheme each tag is initialised with a secret value x_i and two unidirectional functions h_1 and h_2. When a tag receives a request from a reader, it updates the value x_i with the new value obtained from the computation of $h_1^t(x_i)$. Then the tag answers by sending $ID_{i,t} = h_2^t(x_i)$, where i is the tag identifier, t a time step and x_i the updated value. Then, the reader extracts i by an exhaustive search, although to facilitate this operation, the authors propose the use of a threshold m being the aim to reduce the range of values that each tag can send. They also propose the use of a precalculated table $T = ID_{i,t}(i,t)$ where $1 \leq i \leq n$ and $1 \leq t \leq m$ in order to reduce the searching time. Avoine, Dysli and Oechslin in 2005 [6] suggested the idea of using the Hellman's tables [15] as a substitute of the precomputed table T. The main disadvantage of this technique is the desynchronization due to the threshold m, because an attacker can query a tag until reaching the value m. In this case, the tag will be disabled (Denial of Service attack). Moreover, an attacker could distinguish this tag from the others [22]. Some solutions are proposed in [6], one of them is not to answer a reader when it asks more than t times.

3.2 The YA-TRAP Protocol

YA-TRAP (Yet-Another Trivial RFID Authentication Protocol) was proposed by Tsudik in 2006 [28]. This protocol describes a technique for the inexpensive untraceable identification of RFID tags. YA-TRAP involves minimal interaction between devices and a low computational load on the back-end server. With these features, this scheme is attractive for applications where the information is processed in data groups, *e.g.* access points. Using this protocol, each tag is initialised by the next values: K_i that has the function of identifier and cryptographic key, an initial time-stamp value T_0 and a maximum value for the time-stamp range T_{max}. Each tag also contains an iterated keyed hash that is calculated with a secret key and the key K_i. When a reader wants to query a tag, it sends his current time-stamp (T_r). Then the tag verifies the received value. If $T_r \leq T_i$ or $T_r > T_{max}$ the

tag returns a random value. Otherwise, the tag updates T_i with T_r and sends the result of indexing its hash function with T_i. Then, the reader sends T_r to the back-end server and the answer received from the tag. The server queries his database and returns, depending on the query, the meta-ID of the tag, or just whether it is a valid tag. In this protocol the problem of desynchronization of the tag appears again. In [22] some vulnerabilities are pointed out. One of these vulnerabilities arises when an attacker sends a value t_{max} to the tag and uses this value to distinguish two tags. Another vulnerability appears when an attacker sends $t < t_{max}$, where t is far from the current value T_i. In this case the attacker can get access to this tag whilst other readers cannot.

3.3 Deterministic Hash-locks

Weis, Sarma, Rivest and Engels proposed in 2003 the use of hash-locks in RFID devices. A first approach, called *Deterministic hash locks*, was presented in [30]. A tag is usually in a "locked" state until it is queried by a reader with a specific temporary meta-identifier Id. This is the result of hashing a random value (*nonce*) selected by the reader and stored into the tag. The reader stores the Id and the *nonce* in order to be able to interact with the tag. The reader can unlock a tag by sending the *nonce* value. When a tag receives it, the value is checked. Another way of running this scheme is by using some *meta-keys*. Each tag is initialised with a (Id, meta-Key) pair, then, in order to unlock the tag, the *meta-Key* is used. The problem of this solution is the cost of storing these pairs. Note that the Hash approach does not suffer from this shortcoming. Another security problem that must be faced is how to securely send the meta-identifiers from readers to tags and vice versa.

3.4 Improved randomised hash-locks

A recent approach based on Hash-locks can be found in [19], where the *improved randomised hash locks* are presented. The basic operation of the improved randomised hash locks is depicted in Figure 1 and is next briefly described: (i) A reader R sends a challenge c_0 to a tag T, where $c_0 = nonce_R$ is generated uniformly at random. (ii) T generates its own nonce $nonce_T$ and hides its unique identifier ID_T by sending a response $r_0 = (nonce_T, h(nonce_R||nonce_T||ID_T))$. (iii) To determine ID_T, R must perform an exhaustive search of the IDs in its database to compute $r_i = h(nonce_R||nonce_T||ID_{T_i})$ and compare the result with r_0. Once R finds an ID_{T_i} that satisfies $r_i = r_0$, the tag is identified. In [22] it is proved that the improved randomised hash locks offer strong tag privacy in front of eavesdroppers. The main limitation of this technique is its lag of scalability. This technique requires the reader to perform brute-force search to identify tags, which scales poorly. In [27] Solanas et al. provide a solution for this scalability problem.

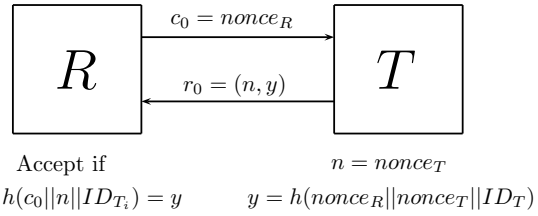

Figure 1: Diagram of the Juels-Weis improved randomised hash locks

3.5 Basic Zero-Knowledge Device Authentication Protocol

This protocol was proposed by Engberg, Harning and Jensen in 2004 [9]. It is based on zero-knowledge protocols which use one-way hash functions and XORs. The main goal of the protocol is that the tag does not need to know its real identity but a shared secret that indirectly identifies it. The protocol works as follows. Initially, the reader[2] sends to the tag

$$[DT, (RSK \oplus h(DT \oplus SSDK)), h(RSK \oplus SSDK)]$$

where DT and RSK are random values and SSDK is the shared secret (owned by the tag and the reader). If the authentication is successful, the tag answers with the response

$$[h(RSK \oplus SSDK \oplus DT)]$$

Note that, if DT is initialised by using a time stamp, the protocol becomes robust against replay attacks. Moreover, the only readers that can access the tag are the ones knowing the shared secret. Last but not least, the communication is performed without revealing any identifier.

3.6 Henrici and Müller Protocol

This protocol was proposed by Henrici and Müller in 2004 [16]. In this protocol there are three main actors: a reader, a tag and a back-end server with a database. The protocol starts with an initialisation phase, in which the tag is initialised with a database identifier (DBID), a random value (ID), a transaction value (TID) and a last successful transaction number (LST) with the same random value. The database also stores the same values. During the authentication phase, when a reader queries a tag, the tag increases its TID and answers the reader:

$$[h(ID), DBID, h(TID \oplus ID), \Delta TID = TID - LST]$$

where $h(ID)$ identifies the tag in the database, $h(TID \oplus ID)$ avoids replay attacks, and ΔTID is used by the

[2] In the protocol it is assumed that the reader is the owner of the tag and that it knows the shared secret.

back-end server to recalculate the current TID. This message is useless to the reader, thus, it must forward the message to the database in order to get access to the desired information. The database verifies the received values and, if everything is fine, it sends the information to the reader. Moreover, a random value (rnd) is generated to compute the new value of the ID of the tag, $ID = rnd \oplus ID$. Finally the database sends a message

$$[rnd, h(rnd \oplus TID \oplus ID)]$$

to the tag by means of the reader. When the tag receives the answer it verifies the values and if they are correct it performs the update. Although the protocol seems to be robust against a number of attacks, in [5] several problems were found.

4 Public-Key in RFID

Most RFID tags have several resource limitations, *e.g.* memory, computational power, etc. that prevent the use of public-key cryptography. On the other hand, strong privacy is a real need that must be achieved, and public-key cryptography seems to be the best way to tackle the problem. Lots of efforts have been devoted to the analysis of public-key protocols and their adaptation to RFID systems. In [29], the authors set out that Elliptic Curve Cryptography (ECC) and Hyper-Elliptic Curve Cryptography (HECC) can be implemented by using less than 5000 gates. Moreover, an implementation of Elliptic Curves (EC) on binary fields using between 12000 and 15000 gates can be found in [7][3]. These public-key-cryptography-based techniques are mainly applied to identification schemes like the Okamoto Identification protocol based on the Elliptic Curves Discrete Logarithmic Problem (ECDLP) [24]. From a different point of view, being the aim to create an unclonable tag, some authors suggest to embed a Physical Unclonable Function (PUF) [8] and to use cryptographic techniques such as digital signatures and secure authentication protocols. Next, we summarise two public-key-cryptography-based identification/verification protocols.

4.1 On-line verification

In an on-line verification, readers share a secret with tags. They must be connected to a database and the number of challenge-response pairs could be large. Batina et al. [8], proposed an on-line verification scheme where the main actors were a reader, a tag and a back-end server (with a database). The back-end server contains a list of Challenge-Response Pairs related to each tag ID. These pairs are computed by using a PUF. The protocol starts with a registration step (*enrolment*), in this step the PUF is challenged by a Certification Authority n times, and the challenges and responses (c_i, x_i) are stored in the back-end server. During the authentication step a reader asks the tag for its ID in order to query the back-end server and it gets the authentication information (*i.e.* a challenge-response pair related to a given ID). Once the reader gets the authentication pair, it sends the challenge to the tag. Then, the tag computes a value y_i by using its PUF based on the Okamoto Identification Protocol [24]. The reader computes the distance $d_H(x_i, y_i)$ and checks whether its result is smaller than a given *threshold*. If this condition is satisfied, the authentication is complete and the back-end server removes the pair (c_i, x_i).

4.2 Off-line PUF-Certificate-Identity based Identification

This off-line verification scheme was proposed in [29]. In an off-line verification, readers are not connected to a back-end. Thus they cannot query a database in order to obtain a Challenge-Response pair. In this scheme the main actors are: (i) a reader and a tag with identity I and a PUF, (ii) a standard identification scheme $SI = (K_g, P, V)$, where K_g is a generation key algorithm, and P and V are interactive protocols that are used by a *Prover* (the tag) and a *Verifier* (the reader), and (iii) a secure signature scheme $SS = (SK_g, Sign, V_f)$ where SK_g is a generation key algorithm, *Sign* is the signature algorithm and V_f is the verification algorithm. The identification scheme $(MK_g, UK_g, \hat{P}, \hat{V})$ is built in two steps (*i.e.* the enrolment and the authentication). During the enrolment step SK_g is used as a master key generation algorithm MK_g to generate a master key msk used to sign and a corresponding public key mpk to verify the signatures. UK_g is an algorithm that creates a public-key pair (pk, sk) for each tag by using the algorithm K_g. The reader interacts with the tag to determine the challenge c for the PUF and the helper data w. In the ROM of the tag w is stored. A certificate $Cert \leftarrow (pk, Sign(msk, pk||I))$ created by the reader is also stored in its ROM. In the authentication step, the algorithms $\hat{P}$ and $\hat{V}$ work as follows. The tag sends $Cert$ to the reader. If $Cert$ is valid, the reader and the tag start the SI protocol. If the tag finishes the protocol without problems, the reader believes that the tag is valid.

5 Conclusions

In this paper we have briefly analysed the most relevant security and privacy protocols for RFID technologies. After introducing the foundations of the technology, we have classified the protocols into three main categories (*i.e.* security in basic tags, security in symmetric-key RFID and security in public-key RFID) in order to provide the reader with a comprehensive reference frame. Although the list of analysed protocols is far from complete, we believe that all the selected protocols are relevant and they

[3]Note that if we compare this number of gates with the one required by symmetric-key cryptography, it is not specially large because *e.g.* optimised implementations of symmetric-key protocols such as AES for RFIDs use about 5000 gates [10].

provide the reader with a proper overview of the security and privacy issues related to the RFID technology.

Disclaimer and acknowledgements

The authors are solely responsible for the views expressed in this paper, which do not necessarily reflect the position of UNESCO nor commit that organisation. This work was partly supported by the Government of Catalonia under grants 2002 SGR 00170 and 2005 SGR 00446, and by the Spanish Ministry of Education and Science under project SEG2004-04352-C04-01 PROPRIETAS.

References

[1] Directive 2002/58/ec on privacy and electronic communications. http://www.dataprotection.ie/documents/legal/directive2002_58.pdf.

[2] Boycott benetton. website, 2005. http://www.boycottbenetton.com.

[3] American Civil Liberties Union (ACLU). RFID position statement of consumer privacy and civil liberties organitzations. website, November 2003. http://www.privacyrights.org/ar/RFIDposition.htm.

[4] G. Avoine. Privacy issues in RFID banknote protection schemes. In *The Sixth International Conference on Smart Card Research and Advances Application - CARDIS*, pages 33–48, 2004.

[5] G. Avoine. Adversarial model for radio frequency identification. *Cryptology ePrint Archive*, 2005/049, 2005.

[6] G. Avoine and P. Oechslin. A scalable and provably secure hash based RFID protocol. In F. Stajano and R. Thomas, editors, *The 2nd IEEE International Workshop on Pervasive Computing and Communication Security - PerSec 2005*, pages 110–114. IEEE, IEEE Computer Society Press, 2005.

[7] L. Batina, J. Guajardo, T.Kerins, N.Mentens, P.Tuyls, and I. Verbauwhede. An elliptic curve processor suitable for rfid-tags. *Cryptology ePrint Archive*, 2006/227, 2006. http://eprint.iacr.org/.

[8] L. Batina, J. Guajardo, T.Kerins, N.Mentens, P.Tuyls, and I. Verbauwhede. Public-key cryptography for RFID-tags. In *Printed handout of Workshop on RFID Security. RFIDSec 06*, pages 61–76, 2006. http://homes.esat.kuleuven.be/~lbatina/Batina_RFID06_2.pdf.

[9] S.J. Engberg, M.B. Harning, and C.D. Jensen. Zero-knowledge device authentication: Privacy and security enhanced RFID preserving business value and consumer convenience. In *Second Annual Conference on Privacy, Security, and Trust*, 2004.

[10] M. Feldhofera, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID system using the AES algorithm. In M. Joye and J. J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, volume 3156, pages 357–370. Springer, 2004. Lecture Notes in Computer Science.

[11] C. Floerkemeier, R. Schneider, and M. Langheinrich. Scanning with a purpose - supporting the fair information principles in RFID protocols. In *Proc. Second International Symposium on Ubiquitous Computing Systems UCS*, 2004.

[12] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets. In T. Okamoto, editor, *RSA Conference - Cryptographers' Track (CT-RSA)*, volume 2964, pages 163–178, 2004.

[13] N. Good, J. Han, E. Miles, D. Molnar, D. Mulligan, L. Quilter, J. Urban, and D. Wagner. Radio frequency identifcation and privacy with informarion goods. In *Workshop on Privacy in the Electronic Society (WPES)*, 2004.

[14] C.C. Haley. Are you ready for RFID? *Internetnews.com*, November 2003. http://www.internetnews.com/wireless/article.php/3109501.

[15] M. Hellman. A cryptanalitic time-memory tradeoff. In *IEEE Transactions on Information Theory*, volume IT-26, pages 401–406, 1980.

[16] D. Henrici and P. Müller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In Ravi Sandhu and Roshan Thomas, editors, *IEEE International Workshop on Pervasive Computing and Communication Security? PerSec 2004*, pages 149–153, Orlando, Florida, USA, March 2004. IEEE, IEEE Computer Society Press.

[17] S. Inoue and H. Yasuura. RFID privacy using user-controllable uniqueness. In *RFID Privacy Workshop*. MIT, November 2003.

[18] A. Juels. Minimalist cryptography for low-cost RFID tags. In *In Fourth International Conference on Security in Communication Networks-SCN 2004*, volume 3352, pages 149–164. Springer-Verlag, 2004. Lectures Notes in Computer Science.

[19] A. Juels. RFID security and privacy: A research survey. Manuscript, September 2005.

[20] A. Juels and R. Pappu. Squealing euros: Privacy protection in RFID-enabled banknotes. In R. Wright, editor, *Financial Cryptography '03*, volume 2742, pages 103–121. Springer-Verlag, 2003. Lectures Notes in Computer Science.

[21] A. Juels, R.L. Rivest, and M. Syzdlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In V. Atluri, editor, *8th ACM Conference on Computer and Communications Security*, pages 103–111, 2003.

[22] A. Juels and S.A. Weis. Defining strong privacy. *IACR eprint*, April 2006.

[23] M. Ohkubo, K. Suzuki, and S. Kinoshita. Efficient hash-chain based RFID privacy protection scheme. In *International Conference on Ubiquitous Computing - Ubicomp, Workshop Privacy: Current Status and Future Directions*, 2004.

[24] T. Okamoto. Probably secure and practical identification schemes and corresponding signature schemes. In E.F. Brickell, editor, *Advances in Cryptology- CRYPTO'92*, volume 740 of *LNCS*, pages 31 – 53. Springer-Verlag, 92.

[25] M. Rieback, B. Crispo, and A. S. Tanenbaum. RFID guardian: A battery-powered mobile device for RFID privacy management. In Colin Boyd and Juan Manuel Gonzlez Nieto, editors, *Australasian Conference on Information Security and Privacy - ACISP 2005*, volume 3574, pages 184–194. Springer-Verlag, 2005. Lecture Notes in Computer Science.

[26] S. E. Sarma, S. A. Weiss, and D. W. Engels. RFID systems, security and privacy implications. Technical report, MIT-AUTOID-WH-014, AutoID Center, MIT, 2002.

[27] A. Solanas, J. Domingo-Ferrer, A. Martínez-Ballesté, and V. Daza. A distributed architecture for scalable private RFID tag identification. *Computer Networks (in press)*, 2007. http://dx.doi.org/10.1016/j.comnet.2007.01.012.

[28] G. Tsudik. YA-TRAP: Yet another trivial RFID authentication protocol. In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*, pages 640–643, 2006.

[29] P. Tuyls and L. Batina. Rfid-tags for anti-counterfeiting. In D. Pointcheval, editor, *Topics in Cryptology-CT-RSA 2006*. Springer Verlag, 2006. Lecture Notes in Computer Science.

[30] S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In W. Stephan D. Hutter, G. Müller and M. Ullmann, editors, *International Conference on Security in Pervasive Computing - SPC 2003*, volume 2802, pages 454–469. Springer-Verlag, 2003.

[31] S.A. Weis. Radio-frequency identification security and privacy. Master's thesis, MIT, June 2003.