An RFID System Based MCLT System with Improved Privacy

Jin Kwak[1,⋆], Keunwoo Rhee[2], Namje Park[2,3], Howon Kim[3], Seungjoo Kim[2], Kouichi Sakurai[1], and Dongho Won[2,⋆⋆]

[1] Faculty of Information Science and Electrical Engineering, Kyushu University, Japan
{jkwak, sakurai}@itslab.csce.kyushu-u.ac.jp
[2] Information Security Group, Sunkyunkwan University, Korea
{kwrhee, skim, dhwon}@security.re.kr
[3] Information Security Research Division, ETRI, Korea
{namejepark, khw}@etri.re.kr

Abstract. Radio Frequency Identification (RFID) systems are increasingly becoming accepted for many EPC Network applications. However, RFID systems have some privacy problems. In this paper, a system for missing child location tracking in the EPC Network applications, is proposed. The proposed system improves security and privacy compared to existing applications, while also keeping in line with traditional procedures, commonly accepted by most industrial applications. The proposed MCLT (Missing Child Location Tracking) system can protect users' privacy while providing location tracking of the RFID tag.

Keywords: EPC Network, RFID system, application service, privacy, security, location tracking.

1 Introduction

The main technology of the EPC Network consists of a RFID system that recognizes and manages RFID tags by use of the Radio Frequency (RF) signal. Low-cost RFID tags can be read, and information can be updated without any physical contact. Therefore, RFID systems have become popular for automated identification in EPC Network applications [8,14,20,23,25]. However, this technology creates new problems, the most important being the invasion of users' privacy. Thus, several methods for protecting the users' location privacy have been proposed [11,12,17,19,21,22,28,29].

However, previous protocols do not resolve security and privacy problems such as location tracking, location history disclosure, and counterfeiting (see [19] for

⋆ The first author was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD). (KRF-2006-214-D00152).

⋆⋆ Corresponding Author: Dongho Won (dhwon@security.re.kr), He was supported by the University IT Research Center Project funded by the Korean Ministry of Information and Communication.

X. Zhou et al. (Eds.): EUC Workshops 2006, LNCS 4097, pp. 579–590, 2006.

more details). In addition, the proposed protocols are not suitable for ubiquitous computing environment, and using distributed databases. In particular, although the RFID tag enables location based applications to be more effective, it may also allow access to information regarding users location, without their agreement. Location based services rely on the availability of user location information. However, location information is sensitive, therefore, releasing this information to random entities may create security and privacy problems. In particular, the previous protocols are not suitable for location based systems for missing child location tracking in EPC Network applications.

In this paper, a system for missing child location tracking using EPC Network applications is proposed. In this proposed MCLT system: (1) the user registers with the registration authority (*RMA* in this paper), (2) the registration authority issues the user with a tag which, for privacy, includes an anonymous-EPC, (3) access to tag information is permitted only by authorized administrators, and (4) for anonymity, the authentication process is performed using a random response at each authentication process between the tag and the reader. In addition, the location of a user can be securely and effectively tracked by authorized administrators, such as in the case of finding a missing child (the tagged user (tag holder)).

The subsequent sections of this paper are organized as follows. After shortly discussing the EPC Network and the associated components in Section 2, security and privacy requirements for the proposed system are presented in Section 3. In Section 4, the EPC Network based MCLT (Missing Child Location Tracking) System is proposed, enabling the protection of users' privacy, while allowing location tracking of the tagged user (tag holder) by authorized administrators when a child is missing. Finally, conclusions are presented in Section 5.

2 The EPC Network

The EPC Network includes several components, the EPC, tag, reader, EPC Information Server (EPCIS), Object Name Service (ONS), and Middleware [1,2,5,6,7,10,16,24].

•**EPC:** The binary representation of the EPC (Electronic Product Code), a combination of *Header*, *EPC Manager*, *Object Class*, and *Serial Number*. *Header* identifies the version, length, tag type, and structure of the code. *EPC Manager* identifies a company, a manager, or an organization. In short, it indicates a manufacturer ID. *Object Class* indicates article classification (manufacturer's product ID). The class number must be unique for all given domains. *Serial Number* is unique for every class and non-repeating for each object class code.
•**EPC Middleware:** EPC Middleware manages EPC data received from the reader, provides alerts, and reads information for communication to the EPCIS (EPC Information Services) or the company's other existing information systems. EPCglobal is developing a software interface standard for services

enabling data exchange between an EPC reader or network of readers and information systems. EPC middleware designed to process the stream of tag data coming from one or more readers, and this particular piece of software manages readers.

•**RFID Tags and Readers:** RFID systems are basically composed of tags and readers. The tag generally consists of an IC chip and an antenna. The IC chip in the tag is used for data storage and logical operations, whereas the coiled antenna is used for communication with the reader. The reader generally consists of an RF module, control unit, and coupling element to interrogate electronic tags via RF communication. The RFID tag is either an active or a passive tag[1]. The EPC is stored on this tag. Tags communicate their EPCs to readers using a RF signal. The readers communicate with tags using the RF signal and deliver information to application systems with EPC middleware.

•**EPC Information Service:** EPCIS (EPC Information Services) enables users to exchange EPC-related data with trading partners through the EPC Network. EPCIS provides EPC Network related data available in PML format to request services. Data available through the EPCIS may include tag data collected from EPC middleware such as date of manufacture, expiry date, and product information.

•**Discovery Service:** The ONS provides a global lookup service, translating EPCs into one or more Internet Uniform Reference Locators (URLs), where further information regarding the object may be retrieved. In short, the ONS provides yellow page services for the EPC Network, allowing participants to quickly discover the server in the EPC Network containing the information associated with a particular EPC. The ONS works same as Domain Name Service (DNS), the foundation naming protocol for the Internet.

3 Security and Privacy Requirements for the Proposed System

In EPC Network applications, especially location based services such as missing child location tracking services, the availability of the users' location information is depended on. However, users usually prefer their location information to be kept secret, because their personal location information is regarded as sensitive. Therefore, only authorized entities should have access to users' location information, and only when necessary [15].

In this section, security and privacy requirements for the proposed system are described. For users' privacy, the EPC of the tag should not be known to the reader or system; only authentication of the tag should be provided. In addition, only authorized administrators should have access to location information, and only when necessary [15].

[1] The *active tag* possesses a battery and actively transmits information to the reader for communication. The *passive tag* must be inductively powered from the RF signal of the reader since RFID tags usually do not possess their own battery power supply. In this paper, the passive tag used to accomplish a hash operation.

Anonymity: The recipient of a response generated by the tag can verify that it is a valid response of the query, but cannot discover which tag created it.
Unlinkability: The recipient of a response generated by the tag can verify that it is a valid response of the query, but cannot be decided whether two responses have been generated by the same tag.
Traceability: The EPC of the tag should be encrypted and stored in a Registration and Management Authority (*RMA*). Location tracking of the tag holder should be possible only through the cooperation of authorized administrators, and only in an emergency situation, such as when a child goes missing.

4 Proposed MCLT System

For the proposed system, the *Registration and Management Authority* (*RMA*) is defined. The *RMA* is a trusted security center managed by a public institution for the registration and location tracking of a user. The *RMA* consists of a *Registration Server* and EPC Network components.

The *Registration Server* issues a tag to the user and stores related information such as telephone number and address of the user in the database. To satisfy security and privacy requirements (see section 3.), the *Registration Server* generates the EID_i (encrypted value of the EPC_i) of the Tag_i. In this paper, for encryption of the EID_i, cryptographic secret sharing methods are adopted [3,4,9,13,18,26,27].

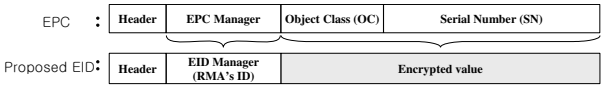

Fig. 1. EID : encrypted value of the EPC

Fig. 1 present *EID* and Fig. 2 presents the proposed system. For the proposed system example, it is assumed that the user travels around three local EPC Network zones in a regular sequence (e.g., school, wear shop, and restaurant zone).

4.1 User Registration

Fig. 3 presents the user registration process for the proposed system.

[Notations and Parameters]

- P : a set of participant Adm_is, $P = \{Adm_1, Adm_2, \cdots, Adm_n\}$
- p : a large prime number, where $p > 2^{512}$
- q : a prime number, where $q \mid p - 1$
- g : an element over $\mathbb{Z}_p$, where $ord(g) = q$
- $Adm_i (1 \leq i \leq n)$: administrators of RMA.

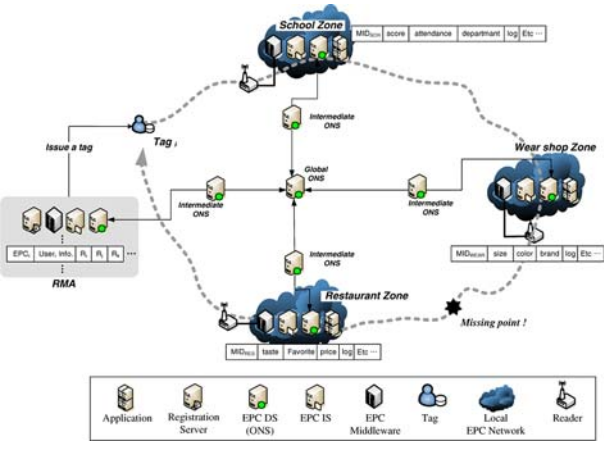

Fig. 2. The EPC Network based MCLT System with Improved Privacy

- y_{Adm} : a group public key of administrators
- $ENC()$: a public key encryption scheme
- $H()$: cryptographically secure hash-functions
- EPC_i : the EPC of the tag$_i$
- EID_i : encrypted value of EPC_i (EID_i=$ENC(EPC_i)$)
- MID_i : meta-ID of Tag$_i$
- ID_i : ID of the local EPC Network
- R_R, R_i : random number chosen by the reader and the tag$_i$

[**User Registration**]

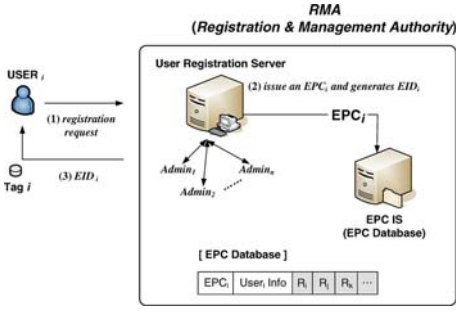

Fig. 3. User Registration for the proposed system

1. User$_i$ make an application[2] for *registration* to *RMA*.
2. *Registration server* in *RMA*,
   (a) issues an EPC$_i$ and then subsequently encrypts it.
   (b) the encrypted value EID_i is written to the Tag$_i$.

[2] For registration, user$_i$ provide information such as an address, telephone number, family exemplification, and so on. The *RMA* stores this information in a database.

(The generation of the Group public key)

① Every administrator ($Adm_i \mid i \in \{1, \cdots, n\}$) selects $r_i \in_R Z_q$ at random and broadcasts $y_i = g^{r_i} \ mod \ p$ to all other administrators in the set S_i.

$$S_i = \{Adm_j \mid j \in \{1, \cdots, n\} \ \ \textbf{AND} \ \ i \neq j\}$$

② To distribute r_i, each Adm_i randomly selects a polynomial f_i of degree $t-1$ in Z_q such that $f_i(0) = r_i$, i.e.,

$$f_i(x) \ = \ r_i \ + \ a_{i,1}x \ + \ a_{i,2}x^2 \ + \ \cdots \ + a_{i,t-1}x^{t-1}$$

with $a_{i,1}, \ \cdots \ , \ a_{i,t-1} \in_R Z_q$, and transmits $f_i(j) \ mod \ q$ to Adm_j in a secure manner ($\forall j \neq i$). Each Adm_i also broadcasts values

$$g^{a_{i,1}} mod \ p \ , \ \cdots \ , \ g^{a_{i,t-1}} \ mod \ p$$

③ From distributed $f_j(i)$ ($\forall j \neq i$), Adm_i checks whether, for each j,

$$g^{f_j(i)} = y_j \cdot (g^{a_{j,1}})^{i^1} \cdots (g^{a_{j,t-1}})^{i^{t-1}} mod \ p$$

④ Let $H = \{Adm_j \mid Adm_j$ is not detected to be cheating at step 3 $\}$. Every Adm_i computes the share s_i secretly, and computes the group public key y_{Adm}.

$$s_i \ = \ \sum_{j \in H} f_j(i) \ \ , \quad y_{Adm} \ = \ \prod_{j \in H} y_j$$

(The encryption of *EPC*)

⑤ To encrypt each EPC_i, Adm_1 picks $t_{i,1} \in_R Z_q$ and computes $g^{t_{i,1}} \ mod \ p$. Then, Adm_1 transmits the result to Adm_2.

⑥ The Adm_2 selects $t_{i,2} \in_R Z_q$ and computes $(g^{t_{i,1}})^{t_{i,2}} \ mod \ p$. Then, Adm_2 transmits the result to Adm_3.

⑦ The final participant $Adm_i (i \neq n)$ computes $g^{t_i} = (g^{t_{i,1}, t_{i,2}, \cdots})^{t_{i,n}} \ mod \ p$ and broadcasts the result to all other Adm_n.

⑧ Through the cooperation of n Adm_i, the ciphertext of EPC_i is generated as follows. Where $\text{OC}\|\text{SN}_i$ is the value of concatenated object class and serial number, detailed in Fig. 1.
$EID_i = ENC(EPC_i) = (g^{t_i}, A), \ where \ \ A = ((y_{Adm})^{t_i} \cdot (OC \| SN_i) \ mod \ p)$

3. The Tag_i is issued to user_i. The Tag_i contains the encrypted value EID_i instead of the EPC_i.

4.2 MID Registration and Tag Authentication

The following steps demonstrate the MID registration and authentication process in each local EPC Network. In this subsection, the registration and authentication processes in the school zone (local EPC Network) are described. The processes of other local EPC Network zones are identical to the processes in the school zone. Fig. 4 demonstrates MID registration and tag authentication in the case of the school zone.

[MID Registration]

The following steps represent the MID registration process in each local Network, through the EPC Network system [7,16]. The detailed protocol of MID registration in the school zone as follows:

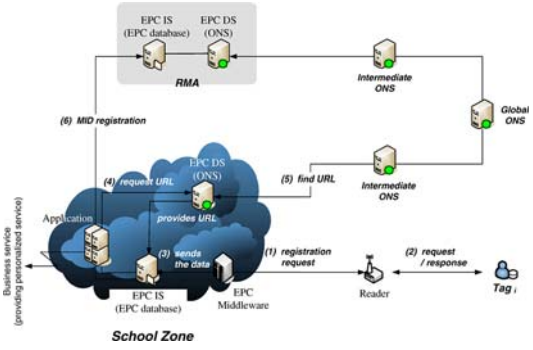

Fig. 4. MID Registration and Tag authentication processes in the School zone

1. The school zone EPC Network system transmits the registration request to the Tag_i.
2. Tag_i generates a random number R_i, and then computes MID_{SCH} and stores it. Then the Tag_i transmits MID_{SCH} to the system. Fig. 5 presents the updated information in the Tag_i.

$$\cdot \text{ tag} \longrightarrow \text{system} : MID_{SCH} = H(EID_i,\ R_i),\ R_i$$

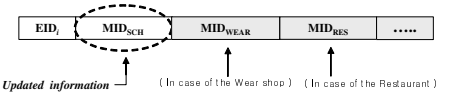

Fig. 5. Updated information in the Tag_i

3. When the local middleware receives data from the Tag_i, the local middleware can be configured to transmit the data further to the local EPCIS. Then local EPCIS stores MID_{SCH} in a database for authentication of the Tag_i.
4. After Step 3, the local EPCIS searches the URL of the Tag_i's issuer for MID_{SCH} registration. In the case where the URL of the Tag_i is unknown to the system, the system will consult the ONS to obtain the URL of the Tag_i.
5. If the local ONS is unable to transform the Tag_i into an URL, the ONS will query other ONS systems higher in the ONS hierarchy, and may potentially make an enquiry to the global ONS via the Internet. The correct URL will then be transmitted to the local EPCIS.
6. Then, local EPCIS transmits the registration message and R_i to the *RMA*. The *RMA* performs a brute-force search to retrieve the EPC; Upon receiving the R_i, the *RMA* calculates MID_{SCH} for all EPC's stored in the database. Only when it finds a match to MID_{SCH} (received from the system) has it identified the right EPC. If the above procedure is successful, the *RMA* stores

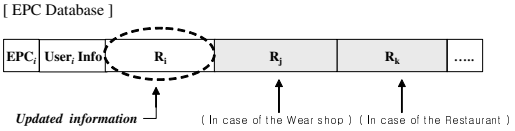

Fig. 6. Updated information of the Tag_i in *RMA*

R_i in their database (see fig. 6-demonstrates how information is updated in the *RMA* for the Tag_i.).

[Tag authentication]

After completing *MID* registration, the local EPC Network performs authentication of the tag [15,19].

Fig. 7 presents the detailed protocol of authentication in the school zone.

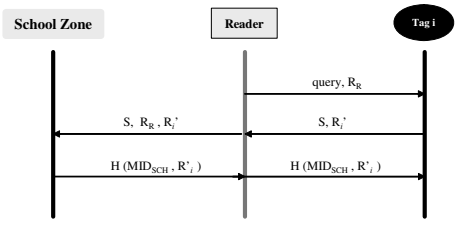

Fig. 7. Tag authentication protocol

① RFID reader transmits a query to the Tag_i with R_R.
② The Tag_i generates random number R_i'. Then the Tag_i computes a response $S(= H(MID_{SCH}, R_i', R_R))$ and transmits it to the reader with R_i'.
③ The reader transmits R_R to the system with S and R_i'.
④ The local EPC Network system computes hash value S' using the stored MID_{SCH}. Then the system subsequently compares it with S, received from the reader to authenticate the Tag_i.

$$\cdot \text{ System : received } S \overset{?}{=} \text{ computed } S'$$

If the authentication is successful, the system transmits $H(MID_{SCH}, R_i')$ to the reader.
⑤ The reader transmits the $H(MID_{SCH}, R_i')$ received from the system to the Tag_i.
Then, to authenticate the system, the the Tag_i computes $H(MID_{SCH}, R_i')$ and compares it with the value received from the reader. If authentication is successful, the system is authenticated.

$$\cdot \text{ tag : computed } H(MID_{SCH}, R_i') \overset{?}{=} \text{received } H(MID_{SCH}, R_i')$$

4.3 Location Tracking Process

In this subsection, the location tracking process in the proposed system in case of finding a missing child, is described. Fig. 8 presents the processes of location tracking the Tag_i.

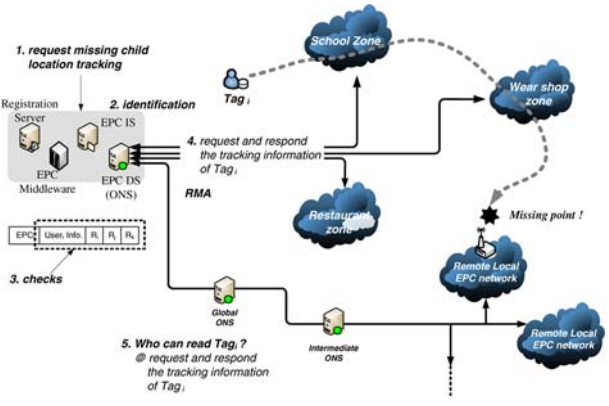

Fig. 8. Missing child location tracking

1. When parents are missing a child, an occurrence of a missing child is reported and location tracking of the tag is requested to the *RMA*. The parents transmit related information (e.g., such as address, telephone number, and family exemplification for verify the identity of the requestor) with a request message.
2. The *RMA* verifies the identity of the requestor using the received information and the stored information in the user registration phase.
3. The *RMA* searches the local EPC Network related specific to the Tag_i. To achieve this step, the *RMA* requires at least t $(n \geq t)$ shared information among n. Since the MID_i is encrypted. Therefore, only authorized administrators can identify the MID_i of the tag_i. If $X = \{Adm_1, Adm_2, \cdots, Adm_t\}$ is a qualified subset to recover the MID_i, the recovery phase is operated as follows;
   - ① Through the cooperation of every $Adm_i \in X$, the value $r_1 + r_2 + \cdots + r_t \bmod p$ is recovered using polynomial interpolation [26].
   - ② Each $Adm_i \in X$ computes $(g^{t_i})^{r_1 + r_2 + \cdots + r_t}$ using a stored g^{t_i}.
   - ③ Each $Adm_i \in X$ computes the EID_i as follows;

$$EID_i = A \;/\; (g^{t_i})^{r_1 + r_2 + \cdots + r_t}$$

4. To retrieve the specific local EPC Network for the Tag_i, the *RMA* computes the meta-ID (MID_i of the Tag_i).

$$\begin{array}{lll} \cdot \text{ computes} & H(EID_i, R_i) & \longrightarrow \; MID_{SCH} \\ \text{computes} & H(EID_i, R_j) & \longrightarrow \; MID_{WEAR} \\ \text{computes} & H(EID_i, R_k) & \longrightarrow \; MID_{RES} \end{array}$$

5. Then, the *RMA* requests the log information of the Tag_i and reads the Tag_i at each local EPC Network. Then the local EPC Network responds to the Tag_i read with a success or failure. If each local EPC Network fails to read the Tag_i, the local EPC Network transmits the log information of the Tag_i to the *RMA*. (see fig. 9)

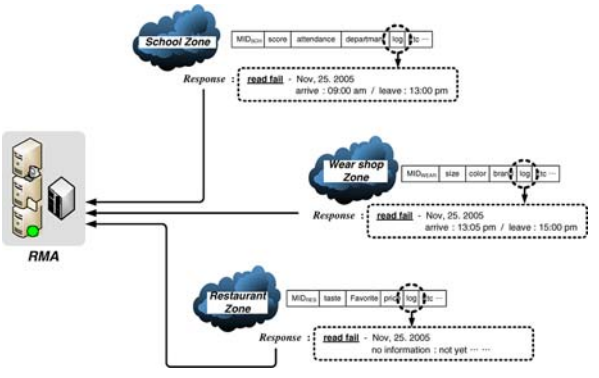

Fig. 9. Response of each local EPC Network

6. After receiving responses, the *RMA* analyzes the received information (see in Fig. 9) and predicts where the child located, in the example below, this is between the wear shop and the restaurant.
7. The *RMA* requests a remote local EPC Network (the local EPC Network of the wear shop, restaurant, and its outskirts) to read the Tag_i via the hierarchical ONS system. If the process does not find a missing child, the *RMA* requests an extension to neighboring districts.
8. Finally, the *RMA* retrieves the location of the missing child successfully. As a result, the missing child is now found.

5 Conclusion

In this paper, a system for missing child location tracking in EPC Networks, with improved privacy, is proposed. In the proposed system, the tag embeds *EID* instead of the EPC, to provide improved privacy for the user. Then registration authority issues tag to the user, which, for privacy, includes an anonymous-EPC.

In conclusion, the following four points are stated: (1) access to the information of the tag is permitted only to authorized administrators, (2) the authentication process is performed using a random response at each authentication process between the tag and the reader, and (3) the location of the tag user can be securely and effectively tracked by authorized administrators, such as, in the case of retrieving a missing child. (4) In addition, although the authorized administrator kept one tag, other tags do not add any security and privacy

problems. Therefore, the proposed system can be satisfied with unlinkability, anonymity and traceability.

Acknowledgement. The 6th author, Kouichi Sakurai, is partially supported by Strategic International Cooperative Program, Japan Science and Technology Agency (JST).

References

1. D. L. Brock. The electronic product code (EPC): A naming scheme for objects. Technical Report MIT-AUTOID-WH-002, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org.
2. D. L. Brock. EPC Tag Data Specification. Technical Report MIT-AUTOID-WH-025, MIT Auto ID Center, 2003. Available from http://www.autoidcenter.org.
3. C. Cachin. On-Line Secret Sharing. Cryptography and Coding: The 5th IMA Conference, LNCS 1025, pp. 190-198, Springer-Verlag, 1995.
4. L. Chen, D. Gollmann, C. J. Mitchell and P. Wild. Secret sharing with Reusable Polynomial. Australian Conference on Information Security and Privacy, ACISP 97, LNCS 1270, pp. 183-193, Springer-Verlag, 1997.
5. D. Engels. The Reader Collision Problem. Technical Report. MIT-AUTOID-WH-007, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org.
6. D. Engels. EPC-256 : The 256-bit Electronic Product Code Representation. Technical Report MIT-AUTOID-WH-010, MIT Auto ID Center, 2003. Available from http://www.autoidcenter.org.
7. EPCglobal. The EPCglobal Network: Overview of Design, Benefits, and Security. 24 September 2004. Available from http://www.epcglobalinc.org.
8. D. M. Ewatt and M. Hayes. Gillette razors get new edge: RFID tags. Information Week, 13 January 2003. Available from http://www.informationweek.com.
9. P. Fedlman. A Practical scheme for Non-interactive Verifiable secret sharing. The 28th Annual Symposium on the Foundation of Computer Science, pp. 427-437, 1987.
10. K. Finkenzeller. RFID Handbook, John Wiley and Sons. 1999.
11. A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFID-enabled banknotes. Financial Cryptography 2003, FC'05, LNCS 2742, pp. 103-121, Springer-Verlag, 2003.
12. A. Juels, R. L. Rivest and M. Szydlo. The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy. 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 103-111, 2003.
13. S. Kim, S. Park and D. Won. Proxy Signatures, Revisited. International Conference on Information and Communications Security, ICICS'97, LNCS 1334, pp. 223-232, Springer-Verlag, 1997.
14. H. Knospe and H. Pobl. RFID Security. Information Security Technical Report, vol. 9, issue 4, pp. 39-50, Elsevier, 2004.
15. J. Kwak, K. Rhee, S. Oh, S. Kim, and D. Won. RFID System wuth Fairness within the frmaework of Security and Privacy. 2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks, ESAS 2005, LNCS 3813, Springer-Verlag, 2005.
16. K. S. Leong and and M. L. Ng. A Simple EPC Enterprise Model. Auto-ID Labs Workshop Zurich. 2004. Available from http://www.m-lab.ch

17. M. Ohkubo, K. Suzuki, and S. Kinoshita. A Cryptographic Approach to "Privacy-Friendly" tag. RFID Privacy Workshop, Nov 2003. http://www.rfidprivacy.org/
18. T. P. Pedersen. A Threshold cryptosystem without a trusted party. Eurocrypt '91, LNCS 547, pp. 522-526, Springer-verlag, 1991.
19. K. Rhee, J. Kwak, S. Kim, and D. Won. Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment. Second International Conference on Security in Pervasive Computing, SPC 2005, LNCS 3450, pp. 70-84, Springer-Verlag, 2005.
20. S. E. Sarma. Towards the five-cent tag. Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org.
21. S. E. Sarma, S. A. Weis, and D. W. Engels. RFID systems, security and privacy implications. Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT, 2002.
22. S. E. Sarma, S. A. Weis, and D. W. Engels. Radio-frequency identification systems. Workshop on Cryptographic Hardware and Embedded Systems, CHES02, LNCS 2523, pp. 454-469, Springer-Verlag, 2002.
23. S. E. Sarma, S. A. Weis, and D. W. Engels. Radio-frequency-identification security risks and challenges. CryptoBytes, 6(1), 2003.
24. T. Scharfeld. An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Identification System Design. MS Thesis, Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, 2001.
25. Security technology: Where's the smart money? The Economist, pp. 69-70, 9 February 2002.
26. A. Shamir, How to share a secret. Communication of the ACM, vol. 21, pp. 120-126, 1979.
27. M. Tompa and H. Woll. How to share a secret with cheater. Journal of Cryptology, vol. 1, pp. 133-138, 1988.
28. S. A. Weis. Radio-frequency identification security and privacy. Master's thesis, M.I.T. May 2003.
29. S. A. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. First International Conference on Security in Pervasive Computing, SPC 2004, LNCS 2802, pp. 201-212, Springer-Verlag, 2004.