12

Evaluation of Group Management of RFID Passwords for Privacy Protection

Yuichi Kobayashi[1], Toshiyuki Kuwana[1],
Yoji Taniguchi[1] and Norihisa Komoda[2]
[1]*Hitachi, Ltd.*,
[2]*Osaka University*
Japan

1. Introduction

The RFID tag is equipped with a small IC tip and antenna, and data can be read from or written to it via radio signal. This device has attracted much attention because it is extremely effective for promoting work efficiency in supply chains and for building IT-based systems connecting companies and/or industries. The scope of RFID use is spreading throughout the entire product life cycle, and RFID is now used not only for primary distribution from production to sale, but also for secondary forms of distribution, such as recycling or maintenance.

The difference between the scope of primary distribution only and the scope of a product's entire life cycle is that in the latter a greater number of general companies and people are involved in the distribution process. Therefore, a provision for protecting data written to RFID tag memory must be included when RFID systems are built so that data cannot be illegally read or overwritten.

In addition, a solution to RFID privacy problems is required so that items with RFID tags can be safely provided to many consumers (CASPIAN et al., 2003; Albrecht & Mcintyre, 2005). We define the privacy problem as unauthorized persons abusing the radio-communications function of RFID tags, and we consider two kinds of privacy problem:

a. Possession Privacy Problem: This is the problem of unauthorized persons or agents being able to surreptitiously detect items that other persons are carrying because of the item codes recorded in the memory of IC tags.
b. Location Privacy Problem: This is the problem of an unauthorized persons or agents knowing where a person is without that person's knowledge because a unique ID is recorded in an IC tag memory.

A guideline for solving privacy problems (GS1 EPCglobal, 2005) states that RFID tags should be removed from products before the products are provided to consumers. However, the requirements for consumers, who want to protect their privacy, conflict with those of industries that want to use RFID tags throughout the entire life cycle of products – satisfying both requirements is very difficult.

To protect consumer privacy, some researchers have proposed systems that mount a hash function in the RFID tag which authenticates interrogators (Weis, 2003; Juels.& Pappu, 2003;

Source: Radio Frequency Identification Fundamentals and Applications, Bringing Research to Practice, Book edited by: Cristina Turcu,
ISBN 978-953-7619-73-2, pp. 278, February 2010, INTECH, Croatia, downloaded from SCIYO.COM

Engberg et al., 2004). However, a hash function has too many gates to satisfy user preferences regarding the size of RFID chips, the communication distance, and the need for an anti-collision algorithm (Satoh & Inoue, 2007). Therefore, mounting hash functions in RFID tags is too difficult at present. We think mounting a function that authenticates the interrogator by using a password is more realistic.

The password authentication function mounted in RFID is standardized by international standards specification ISO/IEC 18000-6 Type C. RFID tags that included a read lock function for privacy protection based on ISO/IEC 18000-6 Type C were developed in the Secure RFID Project (Honzawa, 2008) established by the Ministry of Economy, Trade, and Industry in 2006. To read data in the memory of such RFIDs, authentication of a RFID password requires this read lock function as well as a write lock function. Both these functions prevent illegal reading and writing of the data in RFID memory. However, the security of all RFID tags is compromised when one RFID password is stolen if all the RFID passwords are identical. To reduce the severity of this problem requires setting up a different RFID password for every group of RFID tags.

In this paper, we propose a system for using RFID tags that includes an interrogator with an algorithm that generates RFID passwords. This system sets up the grouping of RFID passwords for RFID tags that are used in the secondary distribution stage, and protects both the RFID data and consumer privacy.

2. Problem with RFID password management for RFID system

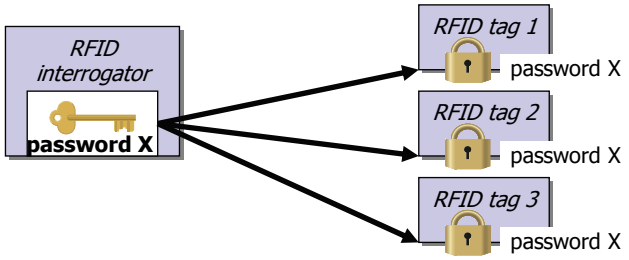
RFID passwords must be managed rigorously to prevent attacks that illegally rewrite data or threaten consumer privacy when data is stored in the memory of RFID tags conforming to the Secure RFID Project specification based on ISO/IEC 18000-6 Type C. If all RFID passwords set in RFID tags are identical throughout an industry, theft of one RFID password will compromise all RFID tags.

To solve this problem, we considered a system that sets up a different RFID password for each group of RFID tags. Although this system does not improve the security of individual RFIDs tags, it narrows the extent of the risk to the whole system. For example, consider the case in which an RFID tag is illegally accessed and its password is stolen. As Fig. 1(a) shows, if the same RFID password, X, has been set to all RFID tags, anyone with the stolen password will be able to access all the RFID tags by using the stolen RFID password X. However, as Fig. 1(b) shows, when a different RFID password is assigned for each group of RFID tags, even if an unauthorized user has stolen the RFID password they can access only one group of RFID tags; the other groups of RFID tags remain safe. Therefore, as few RFID tags have the same RFID password, the damage from a stolen RFID password is contained.

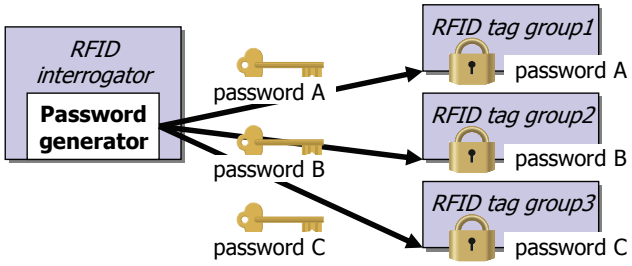
When setting up a different RFID password for every group of RFID tags, though, one has to be careful regarding this privacy protection. For an authorized interrogator to access RFID tags, it must be able to manage the relation between an RFID tag and a RFID password. The identifier of an RFID tag must not be used for invading privacy even though an RFID tag must be discriminable for interrogators to manage the relation between the tags and an RFID password. Therefore, an RFID system used throughout the entire life cycle of a product should satisfy the following requirements:

a. The system must manage the relation between an RFID tag and the grouping RFID password of the RFID tag, and be able to generate a grouping RFID password for the RFID tag immediately after inventorying it.

b. The system must use as little item information as possible for the identifier of RFID tags to protect possession privacy.
c. The system must avoid using unique IDs for the identifier of RFID tags, as much as possible, to protect location privacy.



(a) Common RFID Password



(b) Group RFID Password

Fig. 1. Systems in which interrogators access RFID tags by using RFID passwords

3. An RFID system that generates group RFID passwords

3.1 Group RFID password generation method

An RFID system that generates group RFID passwords only allows authorized interrogators to access RFID tags, and allows those interrogators to read or write data in the RFID memory. Each RFID tag receives an RFID password from an interrogator and authenticates the interrogator; i.e., judges whether the interrogator is authorized for access.

This system sets data called "PASS KEY" for generating a different RFID password for every group of tags, and sets the RFID password as an RFID tag. A group RFID password generation algorithm that finds the right RFID password for each group of RFID tags and sends it to the RFID tag is mounted in an authorized interrogator. The parameters of the grouping RFID password generation algorithm are a master key and a PASS KEY written in an RFID tag.

Figure 2 is a flow chart of the procedure for generating and managing the group RFID passwords.

In the preparation stage, a user chooses a random number as the PASS KEY. The group RFID password generation algorithm calculates this PASS KEY by using a function with collision resistance and pre-image resistance; i.e., a hash function with a master key. The calculation result that this algorithm outputs is used as the group RFID password. The system sends and sets selected PASS KEYs and the generated group RFID passwords to

RFID tags. Since a different PASS KEY is chosen for each group of RFID tags, the RFID password is also set as a different value for each group of RFID tags.

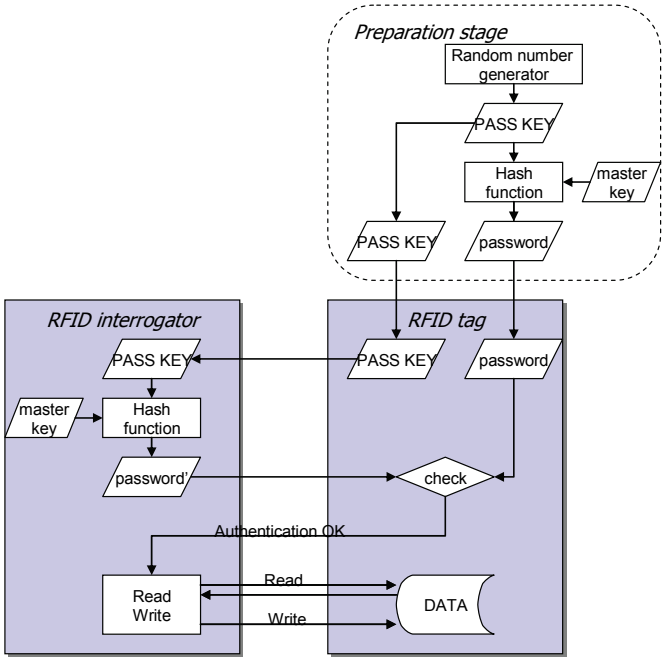


Fig. 2. Procedure for generating group RFID passwords

Whenever a user accesses an RFID tag, the user's interrogator first demands the RFID PASS KEY. The RFID tag receives this demand and reports the PASS KEY to the interrogator. The interrogator first calculates the PASS KEY that it receives from the RFID tag by using a master key and a hash function, and then generates a group RFID password. The interrogator then sends the generated group RFID password to the RFID tag. The RFID tag compares the received group RFID password to the group RFID password that was programmed into it in the preparation stage. If the two RFID passwords are the same, the RFID tag will change to the secured state. When the RFID tag changes to the secured state, the user can read or write to the data in the RFID memory.

Authorized users are not the only ones who can get the PASS KEY from this RFID tag; unauthorized people or agents can also get it. However, since those without authorization do not know the master key, they cannot generate the group RFID password from the PASS KEY, and they cannot read or write to data in the RFID tag.

Generating group RFID passwords requires that the procedure to generate two RFID passwords with the same value from two different PASS KEYs must be made difficult, and decoding a master key from a RFID password and a PASS KEY must also be difficult. Therefore, we adopt a hash function equipped with collision resistance and pre-image resistance as our group RFID password generation algorithm. To construct an RFID system with higher security, an effective method is to use a hash function that has been previously evaluated by the public, such as SHA-1, and to store the master key in a tamper-resistant device.

3.2 Structure of an RFID system with a group RFID password generation method

Here, we provide an example of the structure of an RFID system that uses a group RFID password generation method that sets up and manages group RFID passwords in RFID tags. Figure 3 presents the structure of this system. This system uses RFID tags conforming to the Secure RFID Project specification based on ISO/IEC 18000-6 Type C. The tags are mounted with rewritable memory and an authentication function. The system also includes interrogators, conforming to the Secure RFID Project specification, that communicate with the RFID tags and a tamper-resistant device that restricts users and generates group RFID passwords. The system has middleware that controls the interrogators, the tamper-resistant device, and an RFID application. The middleware and the application can be installed in a terminal. The tamper-resistant device has a user authentication function to prevent unauthorized use of this system and a grouping RFID password generation algorithm that minimizes the damage when RFID passwords are disclosed to unauthorized users.

The user authentication function in the tamper-resistant device applies PIN authentication technology. Users can only use an interrogator after they input an authentic PIN. If they fail to do so, they cannot use an interrogator and cannot access RFID tags. This PIN authentication function can prevent unauthorized use of the interrogator, even if the interrogator is stolen.

The group RFID password generation algorithm is also mounted in the tamper-resistant device, and is processed within this device to prevent leaks and misappropriation of the group RFID password generation algorithm.

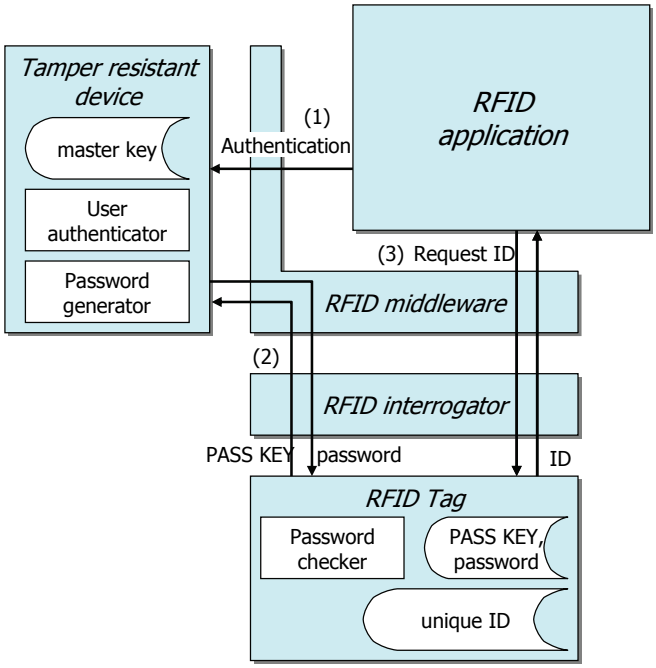


Fig. 3. Structure of system for group RFID password generation

4. Solutions to privacy problems

To protect possession privacy, PASS KEY data should not include any data that identifies items; e.g., an item code or a product number. PASS KEY data should be meaningless data such as a random number. If the PASS KEY is unique and anyone can read it, location privacy is at risk. Moreover, if the PASS KEY of many RFID tags is set up to be identical, many tags will be affected if one RFID password is leaked since the RFID password for every group of RFID tags is also identical. Therefore, some PASS KEYs should be set up as identical to reduce the risk of privacy invasion, and some PASS KEYs must be distributed so that the effects of RFID password disclosure will be limited. We estimated the number of equivalent PASS KEYs that satisfies these two demands by the following methods.
When a PASS KEY is read, the probability of those who are carrying the RFID tag to be specified by that PASS KEY can be calculated as the number of those who can be found out of the entire group carrying an RFID tag that stores identical PASS KEYs. We call this probability the specific probability R.
When we define the number of the tags with the same PASS KEY as the equivalent number M, the specific probability of privacy invasion R can be explained as a reciprocal of the equivalent number M.

$$R = 1/M \tag{1}$$

On the other hand, the influence level of RFID password disclosure, E, when an RFID password is leaked is calculated as the number N of the RFID tags in the market and the equivalent number M, which is the number of tags with the same RFID password.

$$E = M/N \tag{2}$$

Risk, F, is defined as the sum of the weight of the specific probability R and the influence level E. To improve the balance of both specific probability R and the influence level E, we calculate the equivalent number M that provides the lowest risk F. Here, the weight is expressed as w.

$$F = R + wE = 1/M + w\,M/N \tag{3}$$

$$M_{\min} = \sqrt{w^{-1}N} \tag{4}$$

The weight w corresponds to the probability that an RFID password will be leaked.
Figure 4 shows the relations between the probability of privacy invasion R, the influence level of RFID password disclosure E and the risk F. In this figure, we show that if specific probability R is set too low, the risk F become high because the influence level E becomes high. In the following section, we find the effective equivalent number M_{min} in the case of a shopping mall where RFID tags are used.

5. Evaluation of the proposal method's applicability

5.1 Trail analyzing simulation for invasion of location privacy

In this section, we simulate the probability of someone being able to invade a consumer's location privacy in a shopping mall. We assume that consumers carrying items with RFID tags move about in a shopping mall, and unauthorized people or agents secretly install

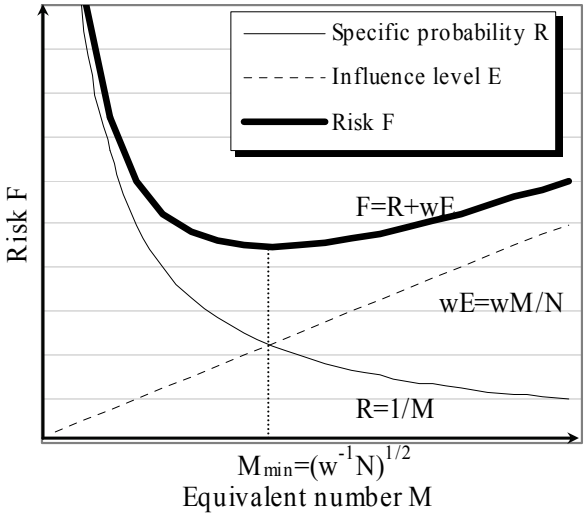


Fig. 4. Balance of both specific probability *R* and the influence level *E*

interrogators and trail consumers by reading the RFID tags. We measure the traceable distance for some equivalent number *M*, and find the equivalent number M_{min} at which the traceable distance becomes the shortest in the case of a shopping mall.

a. Modelling the shopping mall

We assume four models about the shape of a shopping mall as shown in Table 1 and Fig. 5. The floor space of all models is 40,000 m². There is an entrance in the centre of each neighbourhood of the first floor of the shopping mall. In each model, the shopping mall contains 100 stores. Each store's floor space is 225 m² and one interrogator is installed in each store. The width of all passages in each model is 10 m. Each shopping mall always contains 2,000 consumers. A PASS KEY value of an RFID is recorded along with the position and the time when a consumer comes within the readable range of an interrogator, which is 2 m. Model 1 is a 200 x 200 m square within which consumers can move freely because there are no walls dividing stores. Model 2 is a 200 x 200 m square within which consumers move through passages because there are walls separating the stores. Model 3 is a frame type building, around a central courtyard, with a 1,160 m outside perimeter and an 840 m inside perimeter; there is a single passage with stores on both sides. Model 4 is a building with four 50 x 50 m floors where consumers move between floors using a central escalator or one of four elevators.

Model #	Space	Floors	Walls	Entrances	Interrogators	Visitors
1	40,000 m²	1	No	4 sides of 1F	100	2,000
2	40,000 m²	1	Set	4 sides of 1F	100	2,000
3	40,000 m²	1	Set	4 sides of 1F	100	2,000
4	40,000 m²	4	Set	4 sides of 1F	100	2,000

Table 1. Model parameters

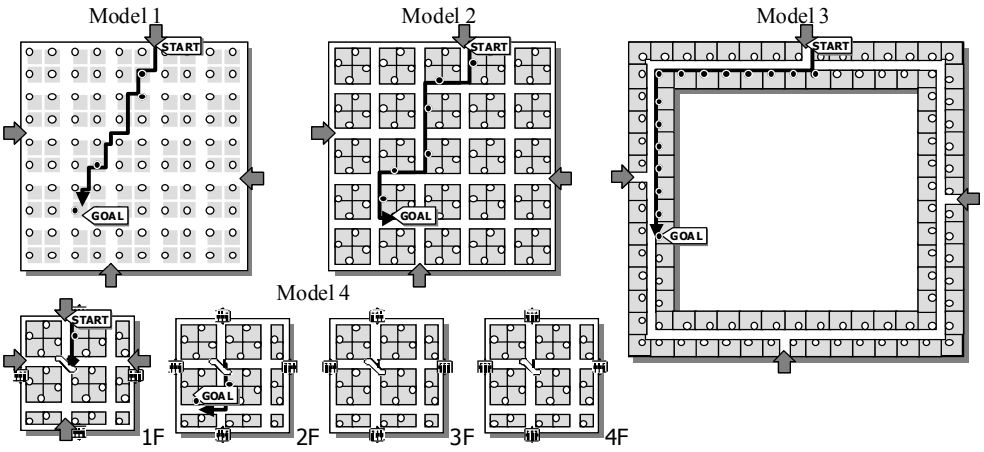


Fig. 5. Types of shopping mall

The consumer movement pattern in this simulation is as follows:

- Each consumer's starting point is randomly chosen from among four entrances.
- The stores to which each consumer goes are chosen at random.
- The number of stores to which each consumer goes varies randomly from 3 to 7.
- A consumer begins by moving to the nearest selected store from the chosen starting point.
- If a consumer arrives at a store, he will stay once and then will move to the nearest selected store from there.
- If a consumer arrives at the last selected store, he will then return to the starting point.
- The time a consumer spends at a store varies randomly from 10 minutes to 30 minutes.
- The distance which a consumer moves in each step is 5 m.
- The speed at which a consumer moves is 1 m/s.

b. Trail analyzing system

This system collects and analyzes log data on the detection of RFID tags with the installed interrogators for consumer trail analysis. The log data consists of an interrogator's ID, the installation position of the interrogator (x, y), a step number, and a PASS KEY value of an RFID. This system creates a consumer's trail by extracting arbitrary PASS KEY values in connection with the consumer out of log data, and sorting these data by time. In this system, there may be some RFID tags with the same PASS KEY values. To trail a consumer as fully as possible, the system disregards data detected at any point at which a consumer cannot physically arrive.

5.2 Result of the trail analyzing simulation

Figure 6 shows a simulation result for the case of five consumers who possess RFID tags with the same PASS KEY value in model 1. This figure shows the route consumer An actually followed and the route for the same consumer observed by the trail analysis system. The routes of the other consumers are also shown. Each white circle indicates an interrogator. In this case, consumer A started from point (110, 10). After moving 135 m, he encountered consumer C at point (90, 130). Therefore, the traceable distance was 135 m since

it became impossible for the trail analyzing system to distinguish consumer A and consumer B after their routes met.

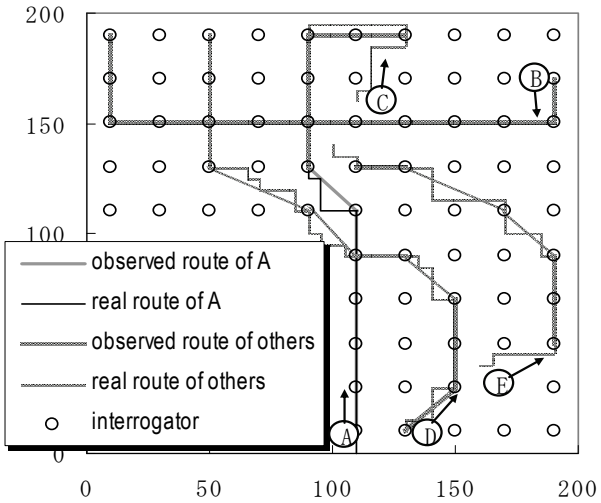


Fig. 6. Flow line analysis simulation result

Figure 7 shows histograms of the traceable distance L acquired through 10,000 simulations when the equivalent number M of PASS KEY was 1, 5, 10 or 20 and the shopping mall type was Model 1. The respective standard deviation was 148, 104, 55, and 27. This figure shows the traceable distance L becomes short if the equivalent number M increases.

Figure 8 shows the average of the traceable distance L as a function of the equivalent number M in each of the four models. When the equivalent number M was 1, the traceable distance L was 817 m; when the equivalent number M was 70, the traceable distance L was 0.9 m. In this simulation there were many consumers possessing RFID tags with the same PASS KEY value, so we know there was a high probability that consumers possessing RFID tags with the same PASS KEY value would meet and these consumers would consequently be hard to trail.

Next, we consider the effect of RFID password disclosure E in this simulation. The influence rate wE when an RFID password is leaked is expressed as follows from equation (2). The probability w of an RFID password being decoded by brute force attack in one year and subsequently leaked is set to 50%. The number N of the RFID tags in the shopping mall is set to 2,000.

$$wE = \frac{0.5}{2000} M \tag{5}$$

The risk F obtained from this simulation result and equation (5) is shown in Fig. 8. (The right vertical axis in the figure shows the rate of risk F). This figure shows that an equivalent number M of about 45 leads to the smallest risk F. When the equivalent number M is 45, the influence level of RFID password disclosure E is about 2% and the traceable distance L is about 3.5 m although the distance which a consumer walked in a shopping mall is 817 m.

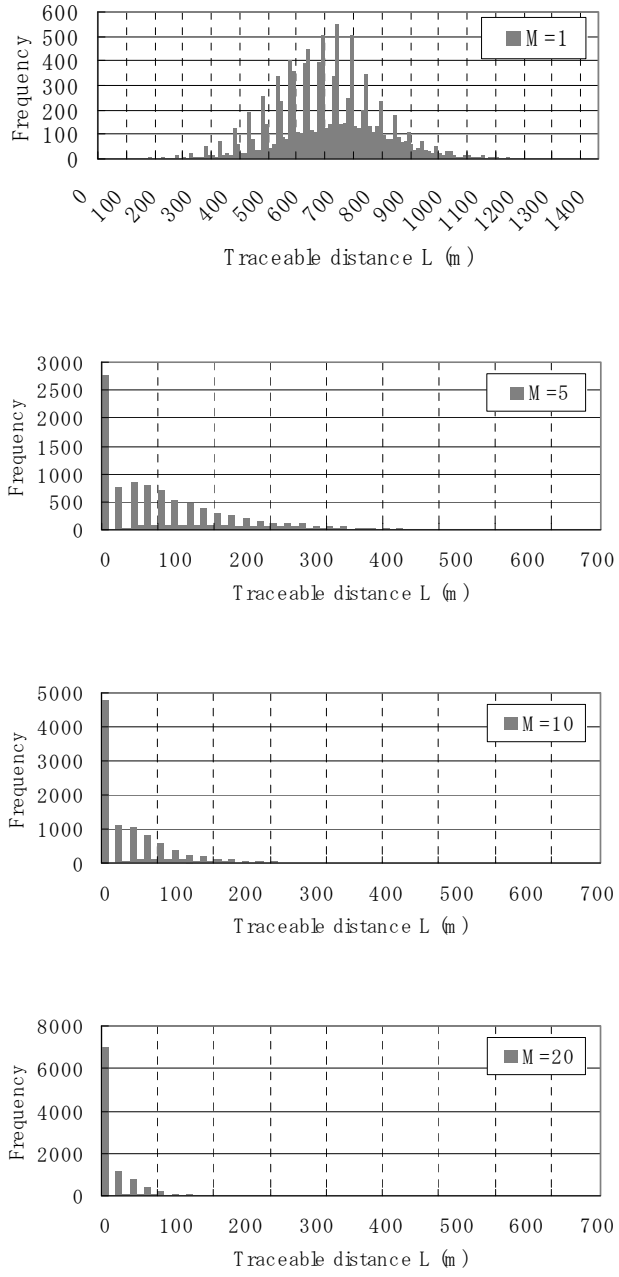


Fig. 7. Traceable distance L in case M = 1, 5, 10 and 20

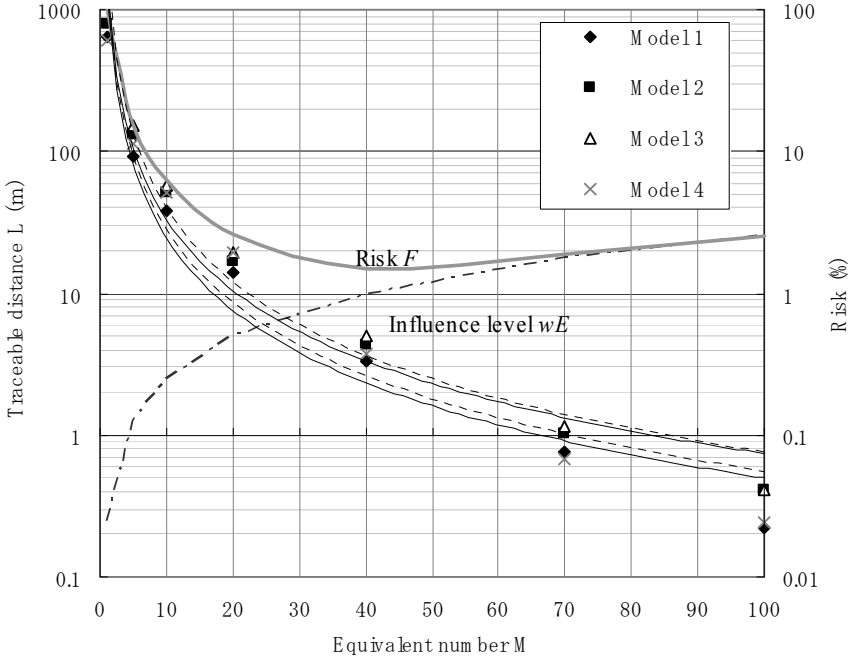


Fig. 8. Traceable distance L vs. the equivalent number M

6. Conclusion

RFID privacy problems will have to be solved before items with RFID tags can be safely provided to consumers on a large scale. Here, we considered the location privacy problem of unauthorized persons or agents being able to trail a person by tracing a unique ID recorded in an attached RFID tag.

We proposed a method for using RFID tags that include an interrogator with an algorithm to generate RFID passwords. This method groups RFID passwords for RFID tags in a way that protects consumer privacy.

We simulated the possibility of trailing a consumer in a shopping mall. We investigated how much the traceability of a consumer changed when the proposed method was applied. Simulation results showed that the traceability fell by about 0.4% when the influence level of RFID password leakage was 2% in this model.

In practice, it may be difficult to read a consumer's RFID tag from distances like those assumed in this simulation because RFID is easily influenced by various environmental conditions. However, even if invasion of privacy is technically difficult, consumers will remain concerned as long as there is any possibility of invasion of privacy through RFID. Therefore, our proposed method will be useful for RFID system application.

7. Acknowledgment

This paper is based on the achievement of a Japanese National Research and development project, the Secure RFID Project that was conducted by METI (Ministry of Economy, Trade, and Industry) for the eight months from August 2006 to March 2007.

8. References

CASPIAN; ACLU; EFF & EPIC (2003). "Position Statement on the Use of RFID on Consumer Products," http://www.privacyrights.org/ar/RFIDposition.htm.

Albrecht, K. & Mcintyre, L. (2005). "*Spychips: How Government And Major Corporations Are Tracking Your Every Move*," Thomas Nelson Inc., 1595550208, Tennessee, USA.

GS1 EPCgloval. (2005). "Guidelines on EPC for Consumer Products," http://www.epcglobalinc.org/public/ppsc_guide.

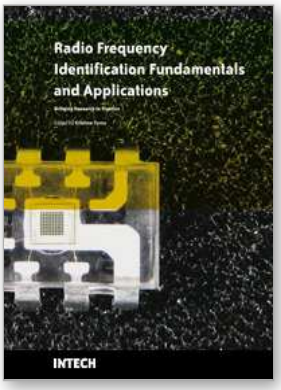
Weis, S. (2003). "Security and Privacy in Radio-Frequency Identification Devices," Masters Thesis, Massachusetts Institute of Technology, Massachusetts, USA.

Juels, A. & Pappu, R. (2003). "Squealing Euros: Privacy-Protection in RFID-Enabled Banknotes," *Proceedings of Financial Cryptography '03*, pp.103-121, Guadeloupe, France.

Engberg, S.J.; Harning, M.B. & Jensen, C.D. (2004) "Zero-Knowledge Device Authentication: Privacy and Security Enhanced RFID Preserving Business Value and Consumer Convenience," *Proceedings of the Second Annual Conference on Privacy, Security and Trust (PST'04)*, pp.89-101, New Brunswick, Canada.

Satoh, A. & Inoue, T. (2007). "ASIC-Hardware-Focused Comparison for Hash Functions MD5, RIPEMD-160, and SHS," *the VLSI journal*, Vol.40, pp.3-10, 0167-9260.

Honzawa, A. (2008). "Secure RFID Project, Spread Use for Product Cycle Management," *Proceedings of GRIFS Workshop*, Halifax, UK.



Radio Frequency Identification Fundamentals and Applications
Bringing Research to Practice
Edited by Cristina Turcu

ISBN 978-953-7619-73-2
Hard cover, 278 pages
Publisher InTech
Published online 01, February, 2010
Published in print edition February, 2010

The number of different applications for RFID systems is increasing each year and various research directions have been developed to improve the performance of these systems. With this book InTech continues a series of publications dedicated to the latest research results in the RFID field, supporting the further development of RFID. One of the best ways of documenting within the domain of RFID technology is to analyze and learn from those who have trodden the RFID path. This book is a very rich collection of articles written by researchers, teachers, engineers, and professionals with a strong background in the RFID area.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821