Privacy for RFID Systems to Prevent Tracking and Cloning

Mala Mitra

Department of Electronics and Communication Engineering, PES Institute of Technology,
100 Feet Ring Road, BSK III Stage, Bangalore, India 560 085.

Summary
Radio Frequency Identification or RFID is finding many applications in our day-to-day life. The system is going to be more popular if the privacy problem can be solved. Apart from data leakage, the technology suffers from tracking of object and cloning of tag problems. Here a review has been done on the existing solutions. A new algorithm with scaleable privacy has been proposed here. Feasibility of implementation and possible attacks and prevention are discussed.

Key words:
Active Attacks, Cloning, Electronic product Code, Encryption, EPC, Radio Frequency Identification, RFID, Security, Tracking,

1. Introduction

RFID is a low-cost solution for object identification and automation [1]. Some of the typical applications are supply chain management, access control, library management, smart appliances [2, 3]. As technology advances, RFID is penetrating more in our day-to-day life. For more widespread applications and to make these systems more popular the security must be enhanced [1, 4, 5,. 6].

One type of security problem is information leakage. For instance, Alice is using a medicine bottle with an RFID tag on it. The tag can give warning at the time of expiry of the medicine. Besides, it eases purchase of another identical bottle with the information available in the RFID tag. Privacy problem may appear along-with all these benefits. Any adversary may interrogate the tag with her tag reader to find out the details of the medicine. The information is enough to find out from which disease Alice is suffering. This is unwanted intrusion to Alice's private life. With this possibility of intrusion, Alice shall prefer to have the medicine bottle without the RFID facility.

This information leakage problem is age-old and common to other wireless systems e.g. internet enabled desktops or laptops, mobile handsets etc. Cryptography is the common solution for this problem. However, implementation of a standard cryptographic algorithm e.g. RSA or ECC [7] needs a good amount of computational facilities: random number generator, arithmetic logic unit or ALU for large numbers etc. RFID tags are low-cost and normally do not have these facilities. Further tags are commonly passive or battery-less and utilizes the reader power. All the computations in the tag should be extremely low power. With these two restrictions, standard cryptographic algorithms were ruled out earlier. Nevertheless, with the advent of VLSI and thrust on low power design more computational facilities are available at passive tags. Thus, computationally intensive asymmetric key cryptographic algorithms are no longer a dream for RFID.

Apart from information leakage, the RFID system suffers from two additional security problems: tracking and cloning [8]. For object / person identification, RFID tag transmits a serial number. The tag responds to any reader without the knowledge of the owner. Any adversary can track that serial number and track the object / person. Standard cryptography e.g. ECC or RSA [7] does not help. An adversary can track the encrypted serial number that remains invariant in all transmissions. Further adversary can get the encrypted serial number and clone another tag with the serial number and can pass wrong information. There are several existing algorithms or protocols to avert these problems. The next section gives a brief discussion on it.

2. Existing Algorithms / Protocols

Yeo and Kwak nicely summarized in their paper in this journal the existing strategies around ISO 18000-6 type C protocol [9]. None of these strategies works against active attack i.e. when an adversary interrogates with her own detector. Authors proposed a new protocol that works against active attack.
In this protocol, the tag transmits its data in EPC when reader interrogates. At the same time, a proxy device transmits a random string of same size as tag data. The random data and tag data creates a collision as shown in Fig. 1.

Without the knowledge on random data, it is not possible to know the tag data from the collided bits. The reader then interrogates the proxy device for the random data.

Manuscript received January 5, 2008
Manuscript revised January 20, 2008

Proxy sends the random number with asymmetric encryption. Only authentic readers have the private key for decryption.

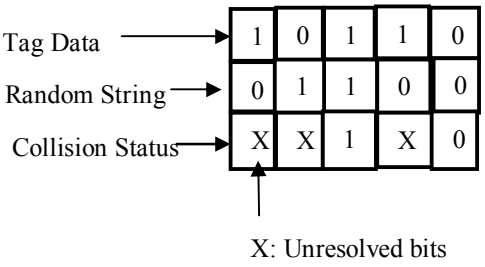

Fig. 1 Privacy Protocol [9]

The protocol is very cost-effective when multiple tags and a single proxy device are used. No change is required in the existing tag architecture. However, multiple active attacks may reveal the tag data. Following gives, a statistical estimate of the number of probable attacks N required for k bit data. In the first interrogation by adversary, the tag and proxy transmit data and random string respectively. For a true randomness, the probability of a bit mismatch is 0.5. The likely number of bit mismatches between tag data and random string and hence the number of unresolved bits in the collision data is k/2. Rests of the k/2 bits are resolved from collision data. In the second attack, the number of mismatches in the unresolved k/2 bits of first run is k/4. In the n^{th} attack, the number of unresolved bits in the collision data is $k/2^n$. If there is one unresolved bit in the collision data at the n^{th} attack, then $k/2^n=1$. Probability of this unresolved bit to be resolved in the next attack is 0.5. With one or two more attacks, this unknown bit is likely to be resolved. The total number of probable attacks N for k bit data:

$$N = n + 0.5 = \log_2 k + 0.5 \qquad (1)$$

As N is a logarithmic function of k the privacy increases slightly with the size of data. However, this estimate is statistical and approximate one for small size data. In this work, the author simulated the number of attacks required for a typical tag data. Data bit length is selected according to the standards of Electronic Product Code or EPC [9]. Random strings are generated based on a Fibonacci series. Time is used as a seed. For a typical tag data size, 12 runs are given to find out the required number of attacks. Table 1 gives the results of simulation.

Table 1: Active Attacks for Yeo and Kwak Protocol [9]

EPC	*Data Type*	*Data Size*	*No. of active attacks, N*			
			Simulation Results	*Frequency*	*Average*	*Statistical Estimate Eqn. 1*
EPC-96	Object Class	24 bits	9	1	5.917	6.08484
			7	3		
			6	3		
			5	4		
			3	1		
EPC-96	Serial Number	36 bits	8	1	6.333	6.670
			7	3		
			6	7		
			5	1		
EPC-258 Type I	Serial Number	192 bits	10	1	8.750	9.085
			9	9		
			7	2		
EPC-258 Type I	Object Class + Serial Number	56+192=248	11	1	8.500	9.454
			10	2		
			9	1		
			8	6		
			7	2		

The result shows that, there is a little gain in privacy with increase in data size.

A. Juel proposed a "minimalist" security model for low cost tags [8] that is very robust for tracking. In this proposed model the tag contains a small collection of pseudonyms. The tag rotates these pseudonyms as identity and releases one against each reader query. An authorized reader can store the full set of pseudonyms in advance and therefore can identify the tag consistently. An unauthorized reader however finds these pseudonyms totally uncorrelated. To protect against frequent attacks to exhaust the pseudonym, the tags slow down their responses or go for a sleep if there are frequent queries. Implementation of this model requires a huge amount of memory and a minimal computational facility. The proposed model in this paper on the other hand requires a good computational facility and a little memory. The recent trend in VLSI shows that, the cost of computational logic is coming down at a faster rate than that of memory.

3. Proposed Algorithm

In this paper, a new security algorithm is proposed, that appears to be resistant against tracking and cloning. Security obtained by this algorithm is scaleable i.e. higher

level of security is possible with more computational facilities.

To implement this algorithm an RFID tag should share a secret key C with an authentic reader. The encrypted identity, E sent by the tag can be given as:

$$E = R * C + I \quad (2)$$

Here I is the identity of the tag. It could be the object class + serial no. in the EPC of the tag. R is a random number. * is multiplication operator. The reader recovers I from E as:

$$I = E(\mathrm{mod})C \quad (3)$$

For successful recovery or decryption, C should be greater than I. An adversary without any knowledge of C cannot recover I from E. This algorithm is resistant to tracking as E varies for active attacks. Cloning is also not possible, as adversary cannot create the correct set of E values without the knowledge of C.

A false detection is possible if secret keys are assigned arbitrarily to the tags. Suppose the secret keys of two tags C_1 and C_2 are related as,

$$C_1 > C_2 \quad (4)$$

Then C_1 can be expressed as:

$$C_1 = nC_2 + m \quad (5)$$

where n and m are two integers or bit strings.
From Eqn. 2:

$$E_1 = R_1C_1 + I_1 \quad (6)$$

Substituting C_1 from Eqn. 5:

$$E_1 = nR_1C_2 + mR_1 + I_1 \quad (7)$$

If for certain R_1:

$$I_2 = mR_1 + I_1 \quad (8)$$

Then Eqn. 7 can be written as:

$$E_1 = nR_1C_2 + I_2 \quad (9)$$

Decryption or recovery follows according to Eqn. 3.

$$I_2 = E_1 \bmod C_2 \quad (10)$$

Then, E_1 may be wrongly decrypted as I_2. To avoid this situation, C_2 should be greater than C_1 if I_2 is greater than I_1. Secret keys may be randomly generated and monotonically arranged. Then, they can be distributed to the tags with monotonically arranged identity numbers.

4. Feasibility of Implementation

To implement this algorithm a random number generator, a multiplier and an adder is required. Low cost passive tags of the RFID system do not have all these facilities in general. With the advent of VLSI design and a thrust on low power design, more computational facilities are expected in low-cost tags. The famous Moore's law [10] states that, the number of transistors in a chip is going to be doubled in every 18 months. Statistics shows that, the law is still valid. With this optimism, we can say that, we are going to get more computational facilities in the tag without hiking its cost.

It is now possible to incorporate an ultra low power microcontroller say, TI MSP430F1232 and implementation of cryptographic algorithm say RC5 is possible [11]. There is a need for an ultra low power cryptographic random number generator that can be integrated to an RFID tag. At present, the reported chips have a power consumption of 3 mW approximately [12, 13]. With the thrust on low power design, this value is expected to come down appreciably.

RFID system works in a multi tag environment. If two or more tags talk at the same time there will be collisions. To avoid these there are two standard protocols (i) Binary Tree and (2) Slotted Aloha [14]. Binary tree protocol is a reader talk first protocol. The reader identifies a tag and the tag responses and passes information. There is a violation of privacy in the protocol itself. On the contrary, slotted Aloha protocol is a tag talk first protocol. Abderrazak et al. gave a very good explanation of slotted Aloha protocol [14]. In this case, time division multiplexing of tag response avoids collision. A reader sends a signal to the tags by a number N that stands for time slots. A tag randomly selects a time slot in-between 1 to N. Reader finds out the number of tag responses in each slot. The reader allows the tag to go for a sleep after successful reading. Modifies the no. of slots, N, and transmit again to get the tag response. The process continues till all the tags are successfully read.

For the proposed algorithm slotted Aloha protocol is more suitable for two reasons: (i) The protocol does not hamper the privacy (ii) the protocol need a random number generator facility that can be reused for the algorithm implementation.

5. Anticipated Attacks

5.1 Attacks on Secret Key C

An adversary can randomly select a key C_R. She can calculate identity values from Eqn. 3. If I matches for two Es, the randomly selected key is the right key. The

probability of such an event reduces as bit size of C is increased.

5.2 Cipher Text Attacks

This is a well-known attack in cryptography. This involves analysis of all encrypted numbers (E). A large number of Es can be arranged in order. The difference of consecutive Es can be arranged. This difference Δ can be expressed as:

$$\Delta = E_1 - E_2 = (R_1 - R_2) * C \qquad (11)$$

If each Δ repeats several times, it shall give the confidence that, the minimum Δ (for $R_1=R_2+1$) has been achieved and minimum Δ = C. The probability of such an event reduces with the random number bit size.

5.3 Attacks on Random Number Generator

This attack has been demonstrated recently on Philips Mifare tags [15]. The attack is possible on any system that uses random number generator and proper care is not taken. With the standard architecture, random number generator does not generate all the bits if it is power starved. Allowing less power from the detector the random number generation can be stopped. In such situation for the present proposed algorithm same E will be transmitted according to Eqn. 2. Then for same E in every transmission the object can be tracked by an adversary. However, it cannot be cloned with just one value of E. Any authentic reader shall expect different E values. To solve the tracking problem, the tag should be configured to go to sleep mode for inadequate power.

5.4 Electro Magnetic (EM) Power Analysis Attacks

By analyzing the power absorbed by the tag during computation, some secrets can be broken. Buysschaert *et al.* demonstrated the attack for elliptic curve cryptographic algorithm [4]. The power consumption depends on number of switching from 0 to 1 and 1 to 0 at any node in the VLSI circuit. If computation is done on a fixed set of numbers, the power consumption becomes synonymous to identity number and an object can be successfully tracked with the tag power consumption.

In the present proposed algorithm, in most of the computations: random number generation, multiplication and addition random numbers are involved. Therefore, the power consumption varies from transmission to transmission.

6. Future Work

A cautious implementation of the algorithm is needed. Implementation should eliminate the possibility of any probable attack from adversary. The proper architecture e.g. FPGA or micro-controller should be decided. The total power consumption and speed of execution need to be estimated.

References

[1] A. Juels, RFID Security and Privacy: A Research Survey, An invited paper, IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, pp. 381-394, February 2006.

[2] R. Das, RFID Forecasts, Players & Opportunities 2007-2017, ED Online and IDTechEx, February 2007. Available at site: http://www.elecdesign.com/Articles/Index.cfm?ArticleID=14840&pg=3 and http://www.idtechex.com/products/en/articles/00000521.asp

[3] A. Agarwal and M. Mitra, RFID: Promises and Problems, Techonline April 2006. Available at site: http://www.techonline.com

[4] P. Buysschaert, E. De Mulder, P. Delmotte, S. B. Örs, B. Preneel, G. Vandenbosch, and I. Verbauwhede, Measuring the Vulnerability of Cryptographic Algorithms, IEEE Potentials vol. 25 no.2, pp. 13-17, March/April 2006.

[5] S. Garfinkel, A. Juels, and R. Pappu, RFID privacy: An overview of problems and proposed solutions, IEEE Security and Privacy, vol. 3 no. 3, pp.34-43, May/June 2005.

[6] S. Weis, S. Sarma, R. Rivest, and D. Engels, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, International Conference on Security in Pervasive Computing, March 2003. Available at site: http://theory.lcs.mit.edu/~sweis/spc-rfid.pdf

[7] D. R. Stinson, Cryptography Theory and Practice, Series Ed. K. H. Rosen, CRC, New York, 2002.

[8] A. Juels, Minimalist Cryptography for Low-Cost RFID Tags, in *Proc. 4th Int. Conf. Security Commun. Netw.*, C. Blundo and S. Cimato, Eds. New York: Springer-Verlag, 2004, vol. 3352, Lecture Notes in Computer Science, pp. 149–164 MIT, AUTOID-WH-014, 2002.
A similar paper available at:
www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs

[9] S. Yeo and J. Kwak, Privacy Enhanced Authentication Protocol for RFID Tag System Security, IJCSNS, International Journal of Computer Science and

Network Security, VOL.7 No.9, pp. 1-6, September 2007.
[10] Articles / Press Releases in Intel Museum. Available at site:
http://www.intel.com/museum/archives/history_docs/mooreslaw.htm
[11] H. Chae, D. J. Yeager, J. R. Smith, and K. Fu, Maximalist Cryptography and Computation on the WISP UHF RFID Tag,.In Proceedings of the Conference on RFID Security, July 2007.
[12] T. Zhou, Z. Zhou, Y. Zhibo; Y. Mingyan; and Y. Yizheng, Design of A Low Power High Entropy Chaos-Based Truly Random Number Generator, IEEE Asia Pacific Conference on Circuits and Systems, APCCAS, pp. 1955-1958, Dec 2006.
[13] M. Bucci, L. Germani, R. Luzzi, P. Tommasino, A. Trifiletti, and M. Varanonuovo, A High-Speed IC Random-Number Source for SmartCard Microcontrollers, IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 50 no. 11, pp. 1373-1380, Nov. 2003.
[14] H. Abderrazak, B. Slaheddine and B. Ridha, Performance Analysis of Aloha Protocol for RFID Communication, IJCSNS, International Journal of Computer Science and Network Security, pp. 80-83, VOL.7 No.12, December 2007.
[15] K. Nohl and H. Plotz, 24C3 Mifare crypto1 RFID completely broken, Posted by E. Phillips, Wireless hacks, Jan 2008. Available at site:
http://www.hackaday.com/2008/01/01/24c3-mifare-crypto1-rfid-completely-broken/

Mala Mitra received her PhD degree from IIT, Bombay, India, M. Tech and B. Tech from Calcutta University, India. Her field of specialization is VLSI Design and Embedded Systems. Presently she is serving as a Professor in the Department of Electronics and Communication Engineering, PES Institute of Technology, Bangalore, India. She has around 20 years of experience. She is actively involved in technological consultancies for industries. Her dream is to bridge the gap between industry and academics.