International Journal of Control Theory and Applications

ISSN : 0974–5572

Volume 9 • Number 40 • 2016

WiGen: Infringement the Privacy and Protection Barriers for Group Key Management in RFID System

Aruna S.[a] D. Anitha[a] Anuska Chatterjee[b] Riya Khan[b] and Riddhi Datta[b]

[a]*Assistant Professor, Department of Software Engineering, SRM University, Chennai.*

[b]*Student, 3rd Year, Department of Software Engineering, SRM University, Chennai.*

Abstract: Though Radio Frequency Identification (RFID) systems have been tremendously used in fields similar to retail and logistics, an extensive variety of applications call for privacy-preserved group key management in RFID systems, which requires a genuine machine to read the RFID tags(reader) and a particular set of tags to distribute one single group key without leaking not even a single private information of person tags. With backscatter communications with plain text in RFID systems, it is extremely exigent to attain privacy-preserved set administration as the reader has to report individual tags in the group with the generated group key by propagation. Through open wireless channels, adversary be able to attain every information exchanging among the reader and tags by eavesdropping or even launch impersonation attacks. In this document, we suggest a pioneering wireless individual group key generation scheme, called WiGen, with which a lawful reader be able to create a group key amid itself and those tags in the required group. By successfully leveraging a Bloom filter, the reader can inform those nominated tags in the cluster without leaking the confidential information of those tags. In addition, with WiGen, together the reader and the group tags be able to verify everyone and accomplish the key contract at the same moment. Additionally, WiGen is extremely light-weighted protocol and can be implemented on existing RFID systems. during concentrated efficiency analysis and recognized testimony of privacy, we confirm that WiGen be able to afford an efficient and burly security for group management applications of RFID systems.

Keywords: *RFID, WiGen, Key Agreement, WISP tags.*

1. INTRODUCTION

Radio Frequency Identification (RFID) technology has been widely used in everyday life. RFID applications, such as classification of tags, batch authentication of tags and access control based on groups, are used nowadays and so group key management needs to be done carefully with a valid reader. Meanwhile, the confidential information of those tags (*e.g.*, ID) should be protected during the group management process. For example, in the application of warehousing services, goods attached with RFID tags can be grouped and managed according to different owners. Instead of checking individual RFID tags one by one across the warehouse, querying the goods status regarding an owner can be more efficient by broadcasting the query with the corresponding group key in this particular case.

To realize private and secure group management in RFID systems, however, is very challenging because of three following reasons:

1. Most tags are passive which means that tags are battery-less. That means that tags need to harvest energy and clock from a reader before responding to the query issued by the reader in the manner of backscatter. So, basically, tags can only "talk" to the reader but cannot communicate with each other, thus disabling any group key agreement protocols.
2. With open wireless channels, tags can be activated and scanned by any malicious interrogator, which incurs many security and privacy threats, such as malicious traceability and tag information leakage [1].
3. Tags are very limited in terms of both storage and computation. In addition, the communication range between tags and the reader is very short. Thus, a group management process is required which is light-weight and can thus be used for group key management.

In the literature, there have been several studies on key generation of wireless devices. For example, many key agreement protocols based on public-key cryptography [2] [3] have been proposed. These protocols can perfectly solve the key generation problem among wireless devices but they also introduce high computational cost. Channel-measurement-based approaches [4] [6] measure communication channels between two wireless devices to generate secret keys using channel correlated random variables. Those schemes need devices to measure channel characteristics such as RSSI values which is not proper for group key generation in large scale RFID systems. As a result, there is no existing successful solution, to the best of our knowledge, to tackling the group management problem in RFID systems.

In this paper, an innovative scheme called Wireless private group key Generation (WiGen) is proposed for private and secure group management in RFID systems. WiGen provides secure group key generation for RFID systems. WiGen will be used for all RFID applications. The core idea is to employ the reader as the group head to generate the group key as tags cannot communicate with each other. It does not broadcast the ID of all tags. Instead the reader broadcasts a vector aggregated on those IDs using Bloom filter [7]. Therefore, every designated tag in the group can be notified without leaking any confidential information of tags. After gathering all the responses from those designated tags, the reader encodes the group key by aggregating the group key with those responses and then broadcasts the result. Finally, every designated tag can correctly decode the result and get the group key. The distinctive features of WiGen are three-fold:

1. It needs no dedicated physical interfaces; thus, all messages are sent over an open wireless communication channel.
2. It can preserve the privacy of tags and it also defends against both passive and active attacks as well.
3. It is very efficient and light-weighted protocol feasible for cheap commercial passive RFID systems.

2. RELATED WORK

The state-of-the-art of key generation schemes can be used for wireless devices can be classified into following categories:

1. **Physical insulation :** Faraday cages [8] are basically made of a metal mesh and can be used to protect communication channels among devices from eavesdropping. Therefore, devices in a Faraday cage can communicate in plaintext. However, it is hard to use a Faraday cage in RFID systems due to its limited space. For example, RFID tags may be attached on large objects like cars and big containers.
2. **Cryptography based :** These rely on key exchange of key agreement protocols based on public-key cryptography, such as Diffie-Hellman [2] or RSA [3]. Those schemes are effective in solving the group management problem but need computation-intensive operations. High computation overhead remains the major obstacle to applying cryptography-based schemes to RFID systems.

3. **Physical Imprinting :** Physical imprinting [9] refers to generating keys based on physical contact. In such a scheme, two devices need some additional hardware to establish a link and exchange secret keys over this link. Physical imprinting schemes, however, are not practical in RFID systems since commercial RFID tags often have no physical interface to establish electrical links.
4. **Shake Them Up :** In this scheme [10], device A can send one secret bit to device B by setting A or B as the source field of a broadcasted packet. In this way, only A and B know whether the source field is correct. An eavesdropper cannot retrieve the secret bit since it cannot figure out which device is the real sender. This solution is low cost but not feasible for RFID systems since to establish a shared key between the reader and a tag will need a great deal of packets. Furthermore, using addresses will also expose the group membership information.
5. **Channel Measurement :** Schemes in these categories [4] [6] measure communication channels and utilize those unique channel characteristics (caused by the environment) between two devices to generate secret keys. Since these channel characteristics will differ at different physical locations, an eavesdropper cannot deduce others' channel signatures. This solution can generate shared keys between a pair of devices but is hard to generate keys for groups. Furthermore, additional hardware is required to measure channels, which is infeasible in RFID systems with simple and naive tags.
6. **Noisy Tag :** A noisy tag which generates noise on channels can be used to help tags and a reader establish shared secret keys in this scheme of key generation. With noise, eavesdroppers cannot identify the secret bits that are sent from another tag to the reader. The main problem using noisy tags in group key generation in RFID systems is that if the noisy tag generates a bit identical to the one from the queried tag, the eavesdropper can identify this bit. Additionally, it is inefficient when the secret key is long. Comparing with existing work, WiGen is a wireless and light-weighted group key generation scheme implementable on cheap RFID systems.

2.1. Adversary Model and Problem Formulation

2.1.1. Adversary Model

There are *two* types of attacks that are possible. They are:

1. **Passive attack :** Eavesdropping on the wireless communication channels between tags and the legitimate reader.
2. **Active attacks :** Inserting sophisticatedly designed messages into the channels to cheat or corrupt an RFID system, such as impersonation, replay and executing bogus protocols. Adversaries cannot discard messages between tags and the reader. The reason is that, in the one-hop communication within a very limited range between the reader and tags, it is very hard for adversaries to hijack messages as a man-in-the-middle.

2.1.2. Problem Model

To realize group management in RFID systems, two functionalities must be provided, namely, group generation and group maintenance. Particularly, in RFID systems, group maintenance operations such as tag joining and leaving can be effectively achieved by generating new groups. This is because tags cannot communicate with each other and therefore all operations have to be handled by the reader. A private and secure group key generation scheme, therefore, becomes the cornerstone of constructing private and secure group management in RFID systems. We define the private and secure group key generation problem as follows:

Definition 1: There are a large number of tags Ti, i =1, ⋯, N, where N is the number of tags in a given RFID system. Each tag Ti shares an individual secret key ki with the reader R. R tries to classify these N tags into M groups. Without loss of generality, we assume that Tj , j = l1, ⋯ , ln will be designated into a group Gl by R, where n denotes the number of tags in Gl.

The main challenges in solving the above problem lie in three-fold.

1. All confidential information exchanged over wireless channels between the reader and tags should not be exposed.
2. With backscatter communication, each tag as well as the reader should achieve key agreement without the need for cooperation between tags.
3. As adversaries can launch active attacks over the wireless communication channels, legitimate tags and the reader should be able to authenticate each other.

2.2. Design of WiGen

2.2.1. Overview

Considering the backscatter communication manner in RFID systems, WiGen employs the reader as the group head to coordinate the group key generation. With this arrangement, WiGen has to let the reader notify each designated tag in the group while preserving any private information of tags at the same time. To this end, instead of directly broadcasting the private keys (or IDs) of all tags in a group, the reader broadcasts a message aggregated on all private keys of those tags using a Bloom filter. After receiving the message, each tag in the system can verify whether itself is designated in the group but cannot infer the membership information of other tags. As a result, all notified tags in the group will respond with an authorized message. Moreover, WiGen must achieve key agreement among the tags in the group and the reader without inter-tag communications. After gathering all the authorized messages from tags, the reader generates the group key by aggregating those authorized messages, encodes the key with the private key of each designated tag, and then broadcasts massages containing the encoded group key. In this way, only designated tags can correctly decode these messages with their private keys and get the group key.

The major advantage of WiGen is that it can provide private and secure group key generation over open wireless channels requiring no extra physical interfaces and it is a very light-weighted scheme in terms of storage and computation requirements on tags. Therefore, WiGen is feasible for the cheap passive RFID systems.

2.2.2. Private and Secure Group Key Generation

An intuitive method to share a group key among group members is for the reader to directly broadcast the group key generated with private keys of designated tags in an RFID communication.

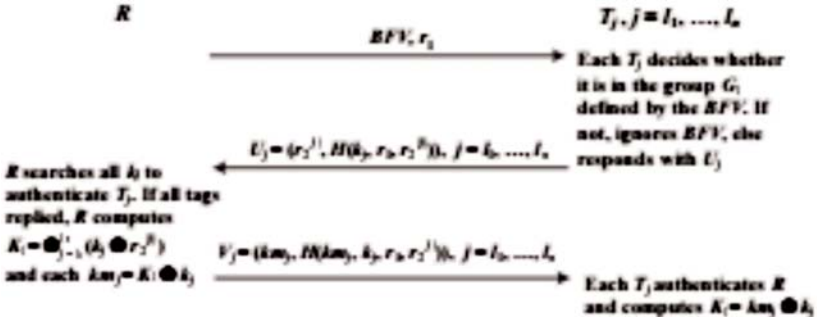

Figure 1: Illustration of the group key generation protocol

The problem of this method is two-fold:

1. Adversary can easily obtain the group key by eavesdropping
2. As there is no mechanism to notify tags which group they belong to, each tag must store all group keys in the system.

With the very restricted memory on tags, the total number of groups in the system is quite limited. Moreover, an adversary can easily overflow the storage of tags by simply broadcasting fake group key. Consequently, it is necessary for the reader to set up a group key only among those designated tags with confidential information of tags preserved and for tags to authenticate the identity of the reader. In WiGen, the group key generation procedure consists of two phases: tag notification and key agreement.

1. **Tag Notification Phase:** As stated in the RFID system model, each tag T_i shares an unique secret key k_i with the reader R. In practice, the unique ID of a tag can be treated as the shared secret key, i.e., k_i is the ID of T_i. To notify tags designated in a group, we leverage a Bloom filter to embed the IDs of all tags in the group. More specifically, if tags T_j , j = l1, ⋯ , ln are to be assigned in the same group G_l, R computes the BFV using a Bloom filter with private keys k_j , j = l1, ⋯ , ln, i.e., BFV = BF (k_j , j = l1, ⋯ , ln). Then, R broadcasts the BFV and a random number r1 to all tags. Upon receiving the BFV and r_1, each tag T_j firstly determines whether it is in the group defined by the BFV. If yes, it picks up a new random number $r^{(j)}_2$ and then replies $U_j = (r^{(j)}_2, H(k_j , r1, r^{(j)}_2))$, where H is a cryptographic hash function (e.g., MD5); otherwise, T_j drops the BFV. With this scheme, only those tags in the group can pass the membership test using the received BFV and get notified. In addition, adversaries cannot infer the group key or any confidential information of tags simply from the BFV.
2. **Key Agreement Phase:** For tags to authenticate the reader and for reader to authenticate tags as well, we design the key agreement phase in WiGen as follows. After notifying group tags, it is essential to achieve group key agreement among tags as well as the reader. Specifically, after receiving Uj , R searches the corresponding private key that can generate H(kj , r1, r(j)2) in the set {kl1 , ⋯ , kln }. Meanwhile, R checks whether all designated tags have responded. If not, R repeats the tag notification phase; otherwise, it computes the group key Kl as Kl = lnj=l1(kj ⊕ r(j)2) for the group Gl. It should be noted that R cannot directly broadcast Kl to all tags as an adversary may be overhearing on the channel. For this reason, R further computes a key material kmj for every Tj as kmj = Kl ⊕ kj , j = l1, ⋯ , ln. At last, R constitutes a message Vj = (kmj , H(kmj , kj , r1, r(j)2)) for Tj and broadcasts all Vj , j = l1, ⋯ , ln. On receiving Vj , Tj firstly computes H(kmj , kj , r1, r(j)2) with its kj as well as the received kmj , and then compares it with the corresponding part in the Vj . If identical, Tj can get the group key Kl = kmj ⊕ kj .The above procedure can effectively achieve not only key agreement but mutual authentication between tags and the reader. For example, only a legitimate tag can generate a valid Uj and only the legitimate reader can generate a valid Vj . We will analyze the impact of the design on the security property of WiGen in Subsection VI-C. The total group key generation procedure is illustrated in Fig. 1.

2.3. Privacy Model

The requirement of the privacy model is that the output of a tag should be independent to that of others regardless of being accessed by valid or invalid interrogators. The independent outputs of tags will make adversaries hard to correlate the current output with previous ones. The model consists of three components: RFID Scheme, Adversaries, and Privacy Game [22].

3. PROTOTYPE IMPLEMENTATION

As normal commercial passive tags cannot be programmed, we implement a WiGen prototype (shown in Fig. 3) with an ImpinJ Speedway Revolution reader (as illustrated in Fig.3) and five Intel WISP4.1 [16] tags which is a passive and programable sensing platform compliant with the EPC C1G2 air interface. We program on the original firmware on WISP tags to support "Read/Write User Memory" commands. In the implementation, we choose to use 64-bit individual private keys and random numbers, which are strong enough against brute-force attacks. We select MD5 with 128-bit output as the hash function to generate messages for the reader and tags.

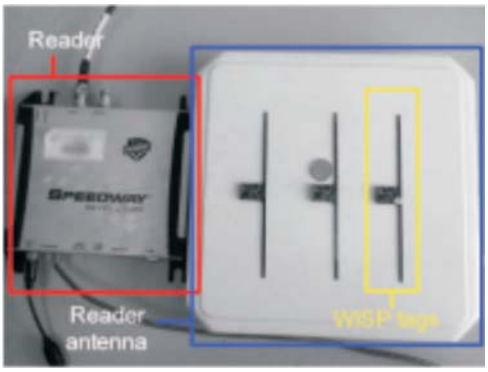

Figure 2: Prototype implementation with WISP tags

The main challenge in implementing WiGen using WISP tags is to solve the energy limitation on tags. For passive tags, the power supply for computation and communication mainly comes from the "Query" signals sent from the reader (see Fig. 2). There are two major factor that determine the energy limitations of a RFID system. The first factor is the operation distance between the reader and a tag as long distance results low signal strength on the antenna of the tag. The second factor is the number of tags in a group. As the reader and tags use certain TDMA scheme to communicate, the reader must access tags sequentially. Therefore, many tags in the interrogation range of a reader cause long waiting time of tags. Moreover, when the reader is writing (reading) messages to (from) a tag, other tags are waiting and listening until receive an acknowledgement or a new "Write/Read User Memory" command. For RFID tags, long time waiting and listening are very energy consuming indeed. Thus, the number of tags which can be accessed by a reader is limited, especially when the reader is writing messages to tags. To overcome the energy limitation, we adopt a multiple inventory scheme (MIS) which slightly modifies the typical writing procedure defined by the EPC Gen 2 standard. In the scheme, when a large message (e.g., a 64-bit long random number) needs to be written into a tag, the message will be divided into multiple short blocks of identical length (e.g., 16 bits). For each block, the reader launches a new inventory which contains a "Query" command to recharge the tag, and then writes the block to the tag in this inventory.

4. PERFORMANCE EVALUATION [22]

We evaluate the performance of WiGen through experiments based on our prototype testbed. From the experience of the prototype implementation, the operation range and the number of tags in a group are two most essential factors having significant impact on the performance of WiGen.

In this experiment, we examine the impact of the distance between the reader and a tag on the performance of WiGen. We change the distance between one WISP tag and the reader from zero to one meter. At each distance, we perform WiGen protocol to generate a group key for this tag and measure the operation time after the tag successfully get the key. We run the experiment ten times and take the average. Fig.4 plots the operation time of WiGen as a function of the operation distance. The operating time first decreases and then increases as the distance increases, and achieve the least operation time at the distance of about 80cm.

The reason is that RFID tag cannot harvest energy efficiently within the distance of $\lambda/2\pi$ due to the inductive effect in the magnetic field [21], where λ is the wave length of RF. The wave length of RFID radio is about 33.3 cm. Thus, within the range of 7 cm the tag needs long time for charging. Out of $\lambda/2\pi$, the tag can get sufficient energy from electric-magnetic fields until the distance is over 80cm, out of which the severe attenuation of the RF power in the air makes tags use longer time to harvest energy. In addition, we can find that the real operation delay is larger than 570ms stated in the discussion section (Section V). The reason is that WISP tags need much more time (about 100 times than normal passive tags [16]) to harvest energy, which therefore causes a long operation delay. Along with more efficient energy harvesting circuits and low-power computation components being adopted, the operation time will also be reduced.

4.1. Impact of the Number of tags

We study the impact of the number of tags in a group on the performance of WiGen. In this experiment, we use MIS to make tags harvest more energy, and change the distance between tags and the reader from zero to 100cm at a step of 5cm. We run the experiment ten times for each setting. Fig.5 plots the operation time as a function of the distance between tags and the reader with different number of tags involved. It can be seen that the operation time increases with the distance and the number of tags. The reason is that more tags need more charging time. In addition,the attenuation of RF also limits the effective charging distance. It can be seen that the operation time is much larger than in Fig. 4.

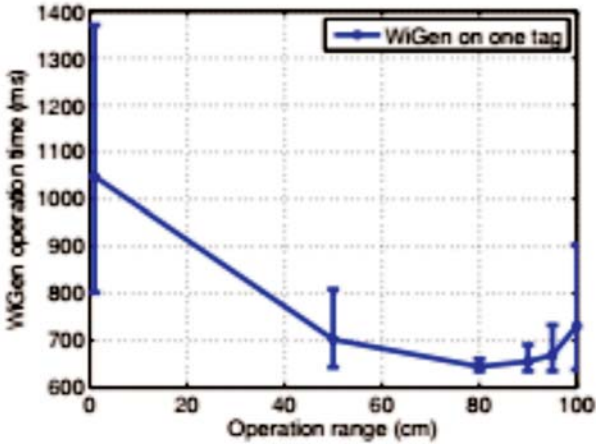

Figure 3: The operation time of WiGen vs the distance between the reader and a tag

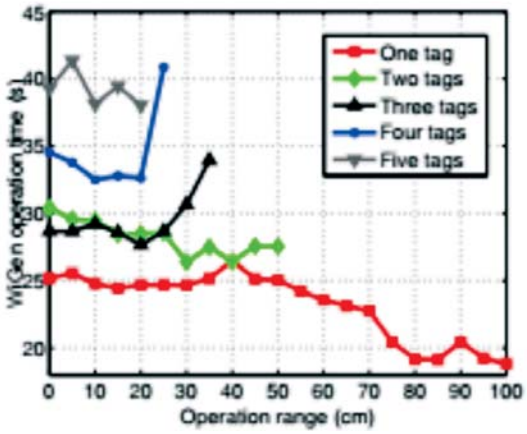

Figure 4: The operation time of WiGen vs the distance between the reader and multiple tags

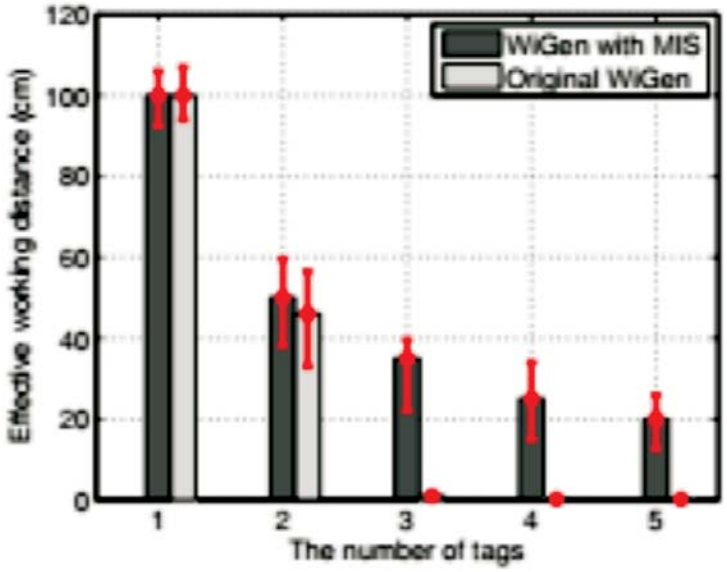

Figure 5: The operation distance of WiGen vs the number of tags in a group

REFERENCES

[1] Ari Juels. RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications, 24(2):381–394, 2006.

[2] Whitfield Diffie and Martin Hellman. Diffie-Hellman Key Exchange. http://en.wikipedia.org/wiki/Diffie-Hellman key exchange.

[3] Christian Genhrmann and Kaisa Nyberg. Enhancements to Bluetooth Baseband Security. In The Nordic Conference on Secure IT Systems, 2001.

[4] P. Bellot and M. Dang. Secret Key Agreement Over a Non-authenticated Channel. IEEE Transactions on Information Theory, 49(4):48–55, 2003.

[5] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. In MobiCom, 2008.

[6] Suman Jana, Sriram Premnath, Mike Clark, Sneha Kasera, Neal Patwari, and Srikanth Krishnamurthy. On the Effectiveness of Secret Key Extraction Using Wireless Signal Strength in Real Environments. In ACM Annual International Conference on Mobile Computing and Networking (MobiCom), 2009.

[7] Knuth Donald. Art of Computer Programming, Volume 3: Sorting and Searching (2nd Edition). ADDISON WESLEY, 2002.

[8] Cynthia Kuo, Mark Luk, Rohit Negi, and Adrian Perrig. Message-In-a-Bottle: User-Friendly and Secure Key Deployment for Sensor Nodes. In ACM Conference on Embedded Networked Sensor Systems (SenSys), 2007.

[9] Frank Stajano and Ross Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In International Workshop on Security Protocols, 1999.

[10] Claude Castelluccia and Pars Mutaf. Shake Them UP! a Movement-based Pairing Protocol for Cpu-constrained Devices. In ACM/Usenix International Conference on Mobile Systems, Applications, and Services(Mobisys), 2005.

[11] Nxp semiconductors, www.nxp.com.

[12] Alien technology, www.alientechnology.com.

[13] Impinj inc., www.impinj.com.

[14] http://www.nfcworld.com/2012/10/31/320871/nxp-launches-new-generation-of-nfc-tags-with-built-in-security-features/. 2012.

[15] James Docherty and Albert Koelmans. Hardware implementation of sha-1 and sha-2 hash functions. In Technical Report in School of Electrical, Electronic and Computer Engineering, Newcastle University. http://async.org.uk/tech-reports/NCL-EECE-MSD-TR-2011-170.pdf, 2011.

[16] Intel Labs Seattle. WISP: Wireless Identification and Sensing Platform, http://seattle.intel-research.net/wisp/.

[17] EPC Global Inc. EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communiations at 860 MHz – 960 MHz, http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2 1 2 0-standard-20080511.pdf.

[18] FAQs UCODE G2X. http://www.nxp.com/documents/application note/an173211.pdf.

[19] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In International Conference on Security in Pervasive Computing(SPC), 2003.

[20] Mihir Bellare and Phillip Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In ACM Conference, on Computer and Communications Security (CCS), 1993.

[21] Inductive Coupling. http://en.wikipedia.org/wiki/inductive coupling.

[22] Li Lu, Muhammad Jawad Hussain and Hongzi Zhu, "WiGen: Breaking the Privacy and Security Barriers for Group Management in RFID Systems", IEEE, 2015.