Security Issues of a Recent RFID Multi Tagging Protocol

Mehmet Hilal Özcanhan
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey

Sezer Baytar
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey

Semih Utku
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey

Gökhan Dalkılıç
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey

***Abstract*—RFID is now a widespread method used for identifying people and objects. But, not all communication protocols can provide the same rigorous confidentiality to RFID technology. In return, unsafe protocols put individuals and organizations into jeopardy. In this paper, a scheme that uses multiple low cost tags for identifying a single object is studied. Through algebraic analysis on chronologically ordered messages, the proposed multi tag arrangement is shown to fail to provide the claimed security. The weaknesses are discussed and previously proven precautions are recommended to increase the security of the protocol, and thus the safety of its users.**

Keywords—Authentication; EPC Gen 2; ISO 18000-6; NFC; RFID; UHF tag

I. INTRODUCTION

Radio Frequency Identification (RFID) is the second widespread tool used in object identification and tracking, after paper barcodes. But, barcodes require a line of sight and can identify only one object at a time. Meanwhile, RFID does not require line of sight and as many as hundreds of objects can be identified within a second [1]. Therefore, it is not surprising to see RFID gradually replacing traditional barcodes in one of the biggest chain stores of the U.S.A. [2]. RFID has also proven itself in analysis of animal behavior [3], anti-counterfeiting [4], business automation [5], asset management [6], and recently in healthcare [7]. Indications are such that RFID will be one of the leading identification tools, in the near future.

Simply, RFID is a set-up of an electronic identification sticker (tag), a reader and a server. The tag has an integrated circuit with a unique identification number (ID) in its memory. An antenna attached to the integrated circuit is used to energize it through electromagnetism. The reader supplies the required electromagnetic energy to activate the tag. After activating the tag, the reader requests the ID of the tag [8]. A tag energized through the reader's electromagnetic field is called a passive tag. Other battery operated tags are called active tags and are not within the scope of the present work. In this study, a special type of passive tags - the low cost Ultra-High Frequency (UHF) tags - that are preferred due to their long reading distance are focused on. Unfortunately, their limited resources cause UHF tags to lack strong security primitives. Capturing the Electronic Product Code (EPC, i.e. the ID) of some tags is very easy [9]. It is possible to track an item with an exposed ID, anywhere it goes on earth [1]. Therefore, it is necessary to look for a standard beyond the security supported in the ISO 18000-6 [10] and EPC Global Class 1 Generation 2 version 2 (Gen-2) [11] standards of the UHF tags. But, it should be noted that high security levels increase the cost of the tags. Therefore, the common goal of the researchers is to obtain a method with a balanced cost – security ratio.

In the rest of this paper, Section 2 summarizes previous work. Section 3 demonstrates weaknesses of a latest proposal. Section 4 contains authentication and security analysis of the proposal and four correction recommendations. In Section 5, the main conclusions and future work are presented.

II. RELATED WORK

Being pervasive yet insecure, early UHF tags have triggered many authentication proposals to be made. The proposals have been categorized according to the functions used for obscuring the tag ID [12]. The proposed protocols are grouped under four categories:

- Ultra-lightweight: Support only bitwise operation functions like AND, OR, XOR ($\oplus$), Shift, Rotate etc.
- Lightweight: Support random number generation and simple functions like cyclic redundancy check (CRC), but not hash functions.
- Simple: Support random number generation and one-way hash functions.
- Fully-fledged: Support conventional cryptographic functions.

Lately, researchers tried to stretch the boundaries between the neighboring categories. The categorization arguments gradually subsided and the attention was turned towards implementation of "lightweight" versions of hash and

cryptographic functions [13]. But, most proposals involve the authentication of a single tag, identifying a single object. There are of course the grouping proof protocols of multiple tags [14], but still each object is identified by a single tag.

Recently, identifying an object with multiple tags based on an ultra-lightweight authentication protocol has been proposed [15]. The proposal will be named Dhal and Gupta's Multi-Tag Authentication Protocol (DGMTAP). DGMTAP places multiple tags on an object as in Figure 1, each with an individual secret shared with the server. As always, the ultimate security goal is preventing the capture of the ID or the shared secret of the tag. The authors claim that DGMTAP resists known RFID attacks of listening adversaries.

Using the notation of Figure 1, *m* number of objects are marked by *n* number of tags. Each tag's index IN_j, shared secret key SK_j (2b bits long), old and new ID_j^{old}, ID_j^{new} are in the server's database. The index provides fast access to the tag record. The protocol assumes that the reader-server channel is secure, but the tag-reader channel is not. Therefore, the attackers can only use r_r (2b bits long), IN_j, M_j, $P1_j$, $P2_j$ that go between the reader and the tags. The equations and functions (Figure 1) used in the protocol are public; therefore available to malicious users as well. The mutual authentication of the server and the tag proceeds as follows: The reader triggers an identification session by sending a request and a random number (nonce) to a tag. Nonces are used for message freshness. No other secret or data is shared with the reader. The server has all the information of the tags in an indexed database, as shown in Figure 1. One or multiple tags receiving the request, prepare their version of message M_j (equation 1), using their own secret SK_j. Next, M_j is sent to the reader preceded by the tag's index IN_j. The reader acts as a mediator to relay the replies of the tags together with its nonce, to the server. Using the index of the tag, the server finds the shared secret key SK_j of the tag and uses it with r_r in equation 2 to extract ($ID_j' - r_j \| r_j$). The apostrophe sign indicates that this is the received value. From here, the concatenated tag nonce r_j is obtained. With r_j, the server calculates ($ID_j^{new} - r_j$) and checks if it equals the received ($IDj' - r_j$) value. If it is a match, the tag is authenticated and the object is identified. If not, the server checks if ($ID_j^{old} - r_j$) equals ($ID_j' - r_j$) value. If it is a match, the tag is authenticated and the object is identified. If not, the tag is rejected. After tag authentication is complete, a new tag $ID_j^{new'}$ is calculated and sent to the tag via the reader, hidden in messages $P1_j$, $P2_j$. The reader merely relays the messages together with the tag index. Tags check the index to decide if the broadcast is intended for itself. If it is, the tag carries out the XOR operation on $P1_j$ (equation 6). Next, the tag obtains tag $ID_j^{new'}$ by adding its own nonce to the result of equation 6 (equation 7). Using $ID_j^{new'}$, the tag analyses message $P2_j$ to verify if the sent ID_j' matches its present ID_j (equations 8 and 9). If it is a match, authentication of the server is complete and the tag saves the new tag $ID_j^{new'}$. The tag finishes and does not acknowledge the server about the completion of mutual authentication.

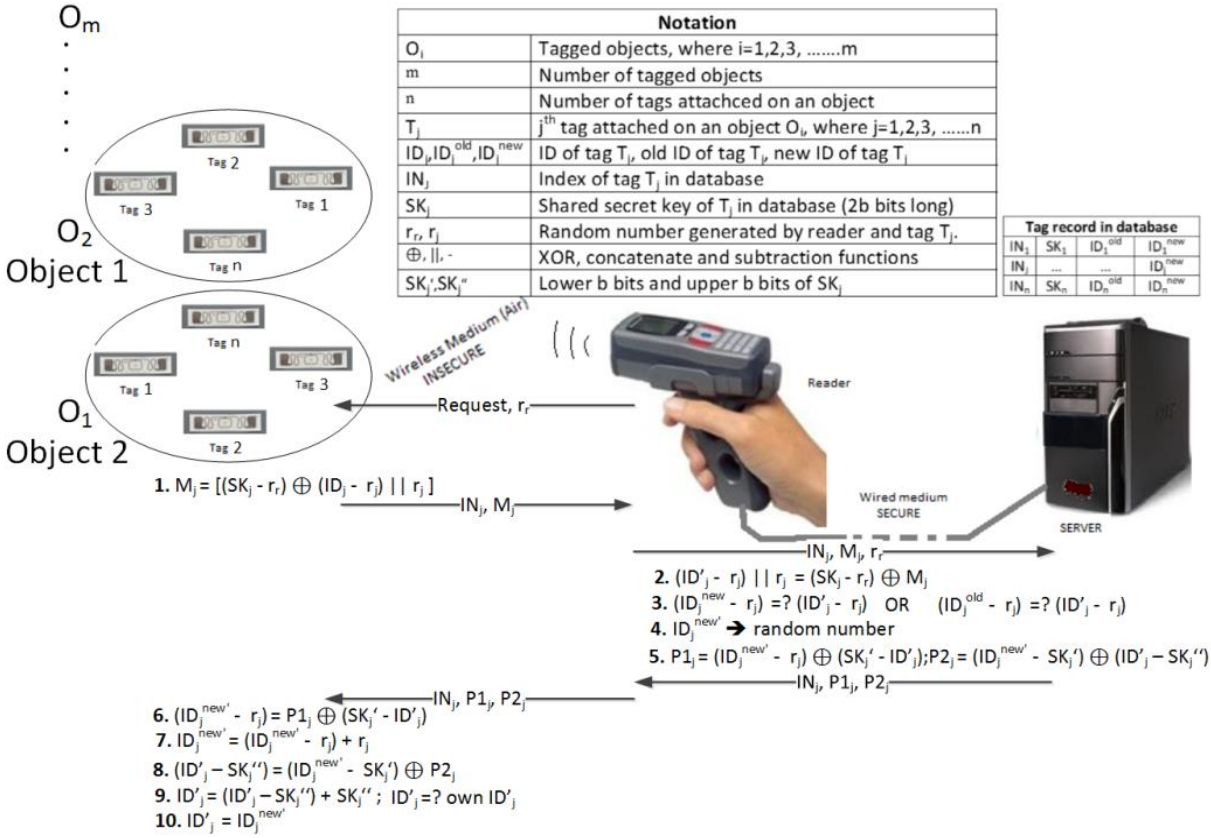

Fig. 1. DGMTAP Scheme (15)

III. ANALYZING DGMTAP

The presence of malicious wireless equipment users and dishonest readers is a common assumption, in radio frequency communications [14]. Adversaries are encouraged especially if a reply to every challenge is guaranteed. Due to the nature of RFID technology, every request is replied by a tag. Therefore, challenging from a distance and recording the replies of a tag is very popular among RFID hackers [16]. The replies are accumulated and analyzed, at a later time. In DGMTAP, although the presence of dishonest readers is assumed and no secrets are shared with the reader; the identity or the nonce (r_r) of the reader are not checked. The absence of the checks opens the way to a serious attack on DGMTAP. As a result of the attack, it becomes obvious that the claimed security properties of the protocol do not exist. Here is the attack scenario in detail:

An attacker challenges the tags of an object using the same bogus nonce $r_c = 0$ twice, and saves the replies. Observe that neither the tag nor the server checks for a zero r_c value. Denoting the first and second challenges with superscripts 1 and 2, respectively, from equation 1 of Figure 1:

$$M_j^1 = [(SK_j - r_c) \oplus ((ID_j - r_j^1) \| r_j^1)] \quad (1)$$

$$M_j^2 = [(SK_j - r_c) \oplus ((ID_j - r_j^2) \| r_j^2)] \quad (2)$$

XORing equations (1) and (2):

$$M_j^1 \oplus M_j^2 = (ID_j - r_j^1) \| r_j^1 \oplus (ID_j - r_j^2) \| r_j^2 \quad (3)$$

Because $(SK_j - r_c) \oplus (SK_j - r_c) = 0$ and $A \oplus 0 = A$. Equation (3) is an XOR operation which can be divided into XORing the lower and upper bits:

$$\text{Upper bits of } (M_j^1 \oplus M_j^2) = (ID_j - r_j^1) \oplus (ID_j - r_j^2) \quad (4)$$

$$\text{Lower bits of } (M_j^1 \oplus M_j^2) = r_j^1 \oplus r_j^2 \quad (5)$$

In mathematics, the XOR function is known as the modulo 2 addition without carry [17]. Therefore, the XOR operation can be approximated to addition. The trivial justification is left to the reader, while the XOR operations on the right hand side of equations (4) and (5) are approximated to addition:

$$UoM = (ID_j - r_j^1) + (ID_j - r_j^2) \quad (6)$$

$$LoM = r_j^1 + r_j^2 \quad (7)$$

Where LoM denotes the Lower bits of $(M_j^1 \oplus M_j^2)$ and UoM denotes the Upper bits of $(M_j^1 \oplus M_j^2)$. Adding equations (6) and (7):

$$LoM + UoM = 2 \times ID_j \quad (8)$$

The ID_j of the tag is obtained using equation (8), since M_j^1 and M_j^2 are passed in cleartext, during the message exchange. Now the attacker has the index IN_j and the ID_j of the tag. Next, the attacker uses the same dishonest reader to send the saved messages M_j^1 and M_j^2 to the server. Observe that, the server never checks the identity or the legitimacy of a reader. The attacker does not allow the replies of the server to reach the tag, but just plays M_j^1 and M_j^2 and saves the replies. The server believes that the tag used IDj′, because it has not updated in the previous authentication session.

Therefore, the server uses the same IDj′ value in its database, for preparing its replies. As a result of the two sessions with the server, the following replies are received by the reader:

$$P1_j^1 = (ID_j^{new1} - r_j^1) \oplus (SK_j' - ID_j') \quad (9)$$

$$P2_j^1 = (ID_j^{new1} - SK_j') \oplus (ID_j' - SK_j'') \quad (10)$$

$$P1_j^2 = (ID_j^{new2} - r_j^2) \oplus ((SK_j' - ID_j') \quad (11)$$

$$P2_j^2 = (ID_j^{new2} - SK_j') \oplus (ID_j' - SK_j'') \quad (12)$$

XORing (9) and (11), then (10) and (11) yields:

$$P1_j^1 \oplus P1_j^2 = (ID_j^{new1} - r_j^1) \oplus (ID_j^{new2} - r_j^2) \quad (13)$$

$$P2_j^1 \oplus P2_j^2 = (ID_j^{new1} - SK_j') \oplus (ID_j^{new2} - SK_j') \quad (14)$$

Approximating the XOR operations in equations (13) and (14) to addition and subtracting (14) from (13) gives:

$$P1_j^1 + P1_j^2 - P2_j^1 - P2_j^2 = 2 \times SK_j' - (r_j^1 + r_j^2) \quad (15)$$

Using equation (7) and rearranging equation (15):

$$2 \times SK_j' = P2_j^1 + P2_j^2 - P1_j^1 - P1_j^2 - LoM \quad (16)$$

All of the terms on the right hand side of equation (16) are cleartext messages saved by the attacker. Therefore, now the lower b bits (notation table of Figure 1) of the shared secret SK_j are captured. The captured values (ID_j and SK_j') can now be used to break down the whole DGMTAP protocol. The attacker returns to equation (1) for a bitwise analysis and since $r_c = 0$, equation (1) reduces to:

$$M_j^1 = SK_j \oplus ((ID_j - r_j^1) \| r_j^1) \quad (17)$$

Separating the upper and lower b bits of the XOR operation, equation (17) can be broken into two equations:

$$UoM_j^1 = SK_j'' \oplus (ID_j - r_j^1) \quad (18)$$

$$LoM_j^1 = SK_j' \oplus r_j^1 \quad (19)$$

From equation (19), the value of r_j^1 is captured, because SK_j' was already exposed. Substituting the captured r_j^1 value in (18), the value of SK_j'' is also obtained. Now, the whole 2b bits of the shared secret SK_j are in the hands of the attacker. Inserting SK_j in equation 2, the second tag nonce r_j^2 is isolated. Now, by inserting the captured r_j^1, SK_j', ID_j' values in (9) and r_j^2, SK_j', ID_j' values in (11); both ID_j^{new1} and ID_j^{new2} are calculated. The tag's record in the database is now completely exposed. The capture of the full record of a tag is called a full-disclosure attack [9] and it has serious ramifications for the user of the tag.

IV. DISCUSSIONS

Authentication protocol proposals are as good as their claims. In other words, when the security of a proposed protocol is proven to be short of what it claims to be, it is immediately abandoned. As demonstrated, full record of DGMTAP tag can be exposed. An exposed RFID tag is not different than a barcode paper sticker on a commodity. The consequences of such a security breach are more critical than just revealing the secret identification of an object, as it will become apparent next.

A. Authentication Analysis

The authors of DGMTAP make four critical errors in their security analysis. First, since the reader - server channel is assumed to be secure, the backend server does not check the authenticity of the reader. The price paid is the giveaway of the two replies to the two bogus messages, in the full disclosure attack demonstrated, in the previous section. Secondly, the number of server replies with the old tag ID is not counted. Thus, blocking the replies of the server can go unnoticed. Hence, the server can be tricked to send multiple replies, using the same tag ID. The adversary simply accumulates the replies and exposes the repeated ID. Third error is the server's failure to check the nonce (r_r) of the reader. As observed in the attack above, a zero valued nonce facilitates the analysis of the DGMTAP messages. Finally, although multiple tags are used to identify an object, each tag's authentication does not add up to a more secure protocol, as in a grouping proof protocol [14]. As demonstrated in our full disclosure attack, the secrets of each tag can be exposed by carrying out the same analysis individually on each tag.

B. Security Analysis

Proposed protocols are normally expected to provide the basic security properties like message confidentiality, message integrity and privacy. Failing to do so, opens the way to the following known attacks.

1) Eavesdropping: Eavesdropping on messages going through air cannot be prevented and contrary to authors' claims, the secrets of DGMTAP tags are not secured enough to go through the air.

2) Man-In-The-Middle Attack: There is no need for this type of attack on DGMTAP, since the secrets can be obtained otherwise. But, after full acquisition of tag secrets, false messages can be formed and the server can be fooled by a man in the middle, using an unchecked dishonest reader.

3) Replay Attack: It has been demonstrated that replaying the same zero-valued reader's nonce, resulted in a full disclosure attack on DGMTAP.

4) Location Tracing: As the present and next identity values of a tag are exposed, by analyzing the exchange between a tag and a reader, an attacker can find out which object a tag belongs to. By recording the locations of the identified objects, tracing an object becomes easy.

5) Forward Security: This property cannot be provided by DGMTAP, because all coming identification values ID_j^{new} of the tag can be calculated, once the shared secret and the present identification ID_j are captured.

6) Backward Security: DGMTAP cannot provide this property, because by inserting the constant value of SK_j and the captured present identification ID_j in the saved message exchanges, all of the old ID_j values can be calculated.

7) Synchronization Attack: This attack is also possible, because a dishonest tag can be created with the captured secrets. The dishonest tag can communicate with the server because it can formulate M_j messages. The server is tricked to update ID_j twice. The authentic tag has no knowledge of the clandestine session between the server and the dishonest tag. Hence, while the identity value in the authentic tag is unchanged, that value has been dropped out of the server's database. Consequently, the server will fail to recognize the authentic tag when it tries to authenticate with the server, because now it has no match in the database.

8) Physical Attack: This type of attack is in another category. Its prevention requires hardware sophistication such as secure memory and memory fuse architectures, which are beyond the scope of this work.

C. Some Recommendations for Correcting DGMTAP

DGMTAP can be improved easily by a number of precautions. First, the server should authenticate the reader and bind its use to a well-proven user. The user must have a secret login password and a unique feature of the reader; like the CPU ID, must be used. A detailed example can be found in work [18]. Such safety precautions eliminate the danger of malicious attacks via dishonest readers. Secondly, the server must check the reader nonce r_r, before evaluating any tag messages. "If $r_r == 0$ ➔ abort" operation would suffice. Such a check eliminates the danger of simplifying the decryption of exchanged messages. Third, a further XOR operation after the concatenation operation in equation (1) can complicate the algebraic analysis of DGMTAP. Concatenation by itself is a weak operation, which can be easily reversed by breaking up a message at the point where it was concatenated. Therefore, concatenation should not be the last operation in an equation. Finally, a grouping proof protocol covering the tags attached on the same object can improve the security, as advised in work [14]. Grouping proof protocols usually challenge the first tag in the group (tag 1), next challenge tag 2 with the reply of tag 1, next challenge tag 3 with the reply of tag 2 and so on. At the end, the replies of the tags are packed and encrypted with the reader's user password. The server receives the resultant data package and verifies the reply of each tag. Any disagreement in the verification causes a fault in the authentication of the chain. Hence, the authentication of the object(s) is dependent on a more sophisticated protocol. DGMTAP has the multi tag basis for a grouping proof protocol, but does not use it.

V. Conclusion

A protocol attempting to bring security to RFID identification by introducing multiple tags per object has been analyzed. Full disclosure of the sensitive tag secrets was possible through an algebraic attack on the exchanged messages. The attack demonstrated that merely multiplying tags for identification can result in the breakdown of the claimed protocol's security features. Four recommendations have been made for improving the security of the analyzed protocol. But, it is best to start with the previous work, recommending lightweight cryptography for RFID tags [13].

Future work must try to comply with the new RFID standards aimed at popular UHF RFID tags [11]. Such intentions lead the research into introducing the Advanced Encryption Standard and Elliptic Curve Cryptography for secure channel initiation, in low cost RFID tags. Strong cryptographic tools are needed even in low cost tags, because

the captured messages are analyzed using computationally powerful computers.

ACKNOWLEDGMENT

This study was supported by TÜBİTAK (The Scientific and Technical Research Council of Turkey) (Project Number: 113S419)

REFERENCES

[1] S. L. Ting, S. K. Kwok, A. H. Tsang and W. B. Lee, "Critical elements and lessons learnt from the implementation of an RFID-enabled healthcare management system in a medical organization," J. Med. Syst, vol. 35(4), pp. 657-669, 2011.

[2] M. L. Songini, "Wal-Mart details its RFID journey," ComputerWorld (April 22, 2007), http://www.computerworld.com/article/2562768/enterprise-resource-planning/wal-mart-details-its-rfid-journey.html (Accessed on 19 December 2014).

[3] J. S. L. Ting, S. K. Kwok, W. B. Lee, A. H. C. Tsang and B. C. F. Cheung, "Design and development of an RFID-based behavioral awareness system for animal care management," Annual Journal of IIE, vol. 27, pp.47-56, 2007.

[4] S. K Kwok, A. H. C. Tsang, J. S. L. Ting, W. B. Lee and B. C. F. Cheung, "An intelligent RFID-based electronic anti-counterfeit system (InRECS) for the manufacturing industry," Proceedings of Seventeenth International Federation of Automatic Control (IFAC) World Congress 2008, pp. 5482–5487.

[5] E. W. T. Ngai, T. C. E. Cheng, S. Au and K. H. Lai, "Mobile commerce integrated with RFID technology in a container depot," Decis. Support Syst, vol. 43(1), pp. 62–76, 2007.

[6] T. Tsuji, S. Kouno, J. Noguchi, M. Iguchi, N. Misu and M. Kawamura, "Asset management solution based on RFID," NEC J. of Adv. Tech., vol. 1 (3), pp. 188–193, 2004.

[7] W. Yao, C. H. Chu and Z. Li, "The adoption and implementation of RFID technologies in healthcare: a literature review," J. Med. Syst, vol. 36(6), pp. 3507-3525, 2012.

[8] M.H. Özcanhan, G. Dalkılıç and S. Utku, "Is NFC a better option instead of EPC gen-2 in safe medication of inpatients," Radio Frequency Identification, Springer Berlin Heidelberg, pp.19-33, 2013.

[9] M.H. Özcanhan, G. Dalkılıç and S. Utku, "Analysis of two protocols using EPC Gen-2 tags for safe inpatient medication," IEEE Innovations in Intelligent Systems and Applications (INISTA), 2013.

[10] Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46149 (Accessed on 19 December 2014).

[11] EPC Global Class1 Gen2 RFID Specifications, http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf (Accessed on 19 December 2014).

[12] H.Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," Dependable and Secure Computing, pp. 337-340, 2007.

[13] M.H. Özcanhan, "Improvement of a Weak RFID Authentication Protocol Making Drug Administration Insecure," Life Science Journal, vol. 11(10), pp. 269-276, 2014.

[14] P. P. Lopez, A. Orfila, J. C. H. Castro and J. C. A. Lubbe, "Flaws on RFID grouping-proofs guidelines for future sound protocols," J. of Network and Computer Appl., vol. 34(3), pp. 833–845, 2011.

[15] S. Dhal and S. G. Indranil, "A new authentication protocol for RFID communication in multi-tag arrangement," IEEE Computing for Sustainable Global Development (INDIACom), 2014.

[16] Y. C. Yen, N. W. Lo and T. C. Wu, "Two RFID-Based Solutions for Secure Inpatient Medication Administration," J. Med. Syst., vol. 36, pp. 2769-2778, 2012.

[17] T. V. Deursen and S. Radomirovic, "Algebraic Attacks on RFID Protocols," Information Security Theory and Practices (WISTP'09), LNCS, vol. 5746, pp. 38-51, 2009.

[18] M.H. Özcanhan, G. Dalkılıç and S. Utku "Cryptographically Supported NFC Tags in Medication for Better Inpatient Safety," J. Med. Syst., vol. 38(8), pp. 1-15, 2014.