ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 1, Issue 5 , December 2014

An Optimized Novel Secure RFID Authentication Protocol against Compromised Tag Attack

T.Parameswaran, Dr.C. Palanisamy, E.Lavanya

Assistant Professor, Dept. of CSE, Anna University Regional Centre, Coimbatore, Tamilnadu, India.

H.O.D, Dept of IT, Bannari Amman Institute of technology, Sathyamangalam Tamilnadu, India.

PG Scholar, Dept. of CSE, Anna University Regional Centre, Coimbatore Tamilnadu, India.

ABSTRACT: RFID (Radio Frequency Identification Device) is increasingly used in all logistic and automation application. But the privacy and security of the system is a big issue while scanning multiple tags. To preserve the privacy and security, number of authentication protocol has been proposed. All these protocols protect the system from all attacks excluding compromised tag attack. In this paper, we demonstrate that the existing system is vulnerable to compromised tag attack. We propose the novel secure RFID authentication protocol based an Elliptic Curve Cryptography (ECC), which prevents the system from compromised tag attack. Also shows that the protocol has the lower reader computational and lower communication cost than Batina and Lee's work, secure ownership transfer protocol (SOTP) and secure multiple group ownership transfer protocol (SMGOTP) while transferring multiple tags.

KEYWORDS: RFID Authentication, Compromised Tag Attack, Elliptic Curve Cryptography, Grouping Proof, Internet of Things

I. INTRODUCTION

Internet of Things (IoT) is a vision of integrated physical and virtual world. RFID is a important part in IoT. RFID is a sensor based technology, which applies the radio signals on products and tracks the information of the objects or living organism. RFID system has two main components called front-end and back-end. The front-end is an embedded IC tags that can be scanned by reader. The back-end is a server that manages all the tag related information. The tag may be a active tag and passive tag. Active tag is a self powered tag. Passive tag is a not a self powered. It gets the power from the external source like reader. Tag related information are tag data and object information. Tag data are tag secret key and unique identifier. Object information is product related information like product name, manufacturer, owner, etc.

Although these object information is not shared the tag data should be shared in secure manner. Valid tag should be authenticated by legal reader. It is simple when authenticates the single tag by single reader. But it is difficult to authenticate multiple tags. The tag and reader privacy should be preserve during scanning the multi tags. The real time examples for this scenario are Pharmaceutical sector, Airport check-in desk, etc. All kind of security threats are faced during scanning multi tags. There is plenty of research going on for these security threats for past six decades.

Sato and Mitsugi proposed 'group coding' which verifies the integrity of the group tag. It finds the number of missing tags. Fornaciari and Cucchiara proposed a camera and RFID mingle method which manages conflicts and uncertain data among multi tags. Yang proposed SMGOTP which performs mutual authentication among tags, reader and verifier. Batina and Lee developed the RFID authentication protocol based on elliptic curve cryptography called privacy preserving multipliers grouping proof protocol. Although their protocol has the resistance to eavesdropping, replay attack and message modification, they are resists the compromised tag attack.

Our proposed scheme main contributions are (a) propose novel secure group RFID authentication protocol (b) analyze the scheme by formal analyse, provable security and mathematical inductive method (c) and compare our scheme with batina, SOTP and SMGOTP scheme.

II. RELATED WORK

Let us introduce ID transfer scheme and notation for this work. Here P is the base point on an elliptic curve, y is the private key of the verifier and Y= yp is the public key of verifier. yp is the point multiplication operation of the EC group and x(T) is the x-coordinate of EC point T. s_t is the private key of the tag t and $S_t = s_tP$ is the Public key of the tag t.

A. ID-Transfer Scheme

The ID transfer scheme between the tag and reader is shown in Fig. 1.In which a tag selects the random value r_{t1} where $r_{t1}\epsilon_R$ Z. A tag computes T_1=r_{t1}P by multiplying EC base point P with the random value rt1. A tag sends the computed value T_1 to the reader. The reader produces the random challenge r_{s1} where r_{s1} ϵ_R Z and sends it to tag. Using this random challenge rs1 and its private key x1, the tag generate T_2=(r_{t1} + $r_{s1}x_1$)Y. Now the reader sends this T_2 to the verifier.

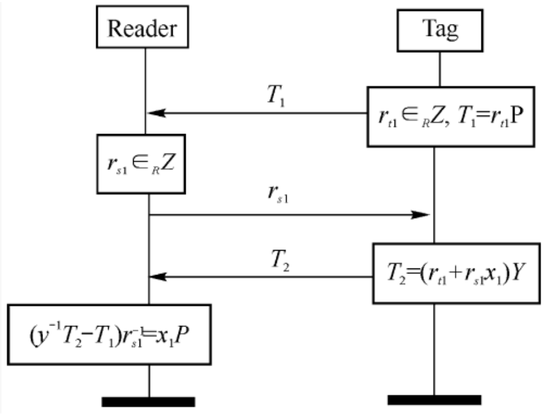
Reader
Tag
T_1
$r_{t1}\in_R Z$, $T_1=r_{t1}$P
$r_{s1}\in_R Z$
r_{s1}
T_2
$T_2=(r_{t1}+r_{s1}x_1)Y$
$(y^{-1}T_2-T_1)r_{s1}^{-1}=x_1P$

Fig. 1 ID-transfer scheme

Verifier calculates,
$x_1P(=X_1)=(y^{-1}T_2-T_1)y^{-1}s_1$, and verify the tag with registered tag value in the reader.

B. ECC-based grouping proof protocol

Assume that there are two tags such as tag A and tag B and they have been scanned simultaneously. Fig.2 shows this illustration. The 2-party CTP protocol is used to detect and solve the collisions. The execution of the protocol as follows.

a. The reader sends “start left” to tag A. It selects the random value r_a ϵ_R Z and calculates $T_{a,1}$=r_aP. This $T_{a,1}$ value is forwarded to the reader.
b. The reader selects the random vale r_s. This r_s and $T_{a,1}$ is forwarded to the tag B.
c. Upon the reception of r_s and $T_{a,1}$, tag B generates the random value r_b and calculates $T_{b,1}$=r_bP and the response $T_{b,2}$=[r_b + x($r_sT_{a,1}$)s_b]Y. Here s_b is a private key of tag B.
d. And this both values are forwarded to the reader.

e. The reader forwards $T_{b,2}$ to tag A. It computes $T_{a,2}$ = [r_a + x($T_{b,2}$)s_a]Y by using the value of $T_{b,2}$ and its private key s_a. $T_{a,2}$ is forwarded to the reader.
f. The reader hands down all the proof collected from tag A and tag B to the verifier.

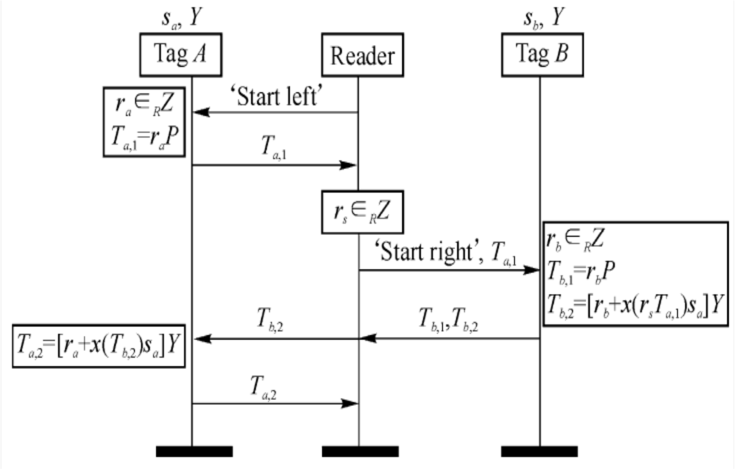

Fig. 2 ECC-based grouping proof protocol

Verifier calculates,
$s_aP = (y^{-1}T_{a,2} – T_{a,1})[x(T_{b,2})]^{-1}$
$s_bP = (y^{-1}T_{b,2} – T_{b,1})[x(r_sT_{a,1})]^{-1}$
The verifier checks whether the public key of the tag A and tag B is registered at the verifier database. If it is accepted, time stamp is added. This protocol can be extended to multiple tags.

C. Compromised Tag Attack (CTA)

The two party CTP protocol works as follows. In which tag A and tag B are scanned simultaneously using session.

a. At the session S_1 the reader sends "start left" to tag A. Tag A selects random value $r_a \epsilon_R$ Z and calculates the $T_{a,1} = r_aP$. And then $T_{a,1}$ is forwarded to reader.
b. Reader selects the random value $r_s \epsilon_R$ Z and forwards this to tag B.
c. Now the attacker starts the session S_2 before S_1 is completed. Attacker selects the random value $r_a \epsilon_R$ Z and computes $T_{a,1} = r_aP$ and forwards them to reader.
d. Now the reader selects $r_s’\epsilon_R$ Z and corrupts the tag B as follows.
e. Tag B sets $r_b = x(r_s’T_{a,1})s_b$ and computes $T_{b,1} = r_bP$, $T_{b,2} = [r_b + x(r_sT_{a,1})s_b]Y$. And then forwards them to tag A through reader.
f. Tag A computes $T_{a,2} = (r_a + x(T_{b,2})s_a]Y$ and forwards them to the reader. The reader hands down all the proof collected from tag A and tag B to the verifier.

Verifier calculates,
$S_aP = (y^{-1}T_{a,2} – T_{a,1})[x(T_{b,2})]^{-1}$
$SbP = (y^{-1}T_{b,2} – T_{b,1})[x(r_sT_{a,1})]^{-1}$
The verifier checks whether the public key of the tag A and tag B is registered at the verifier database. Now the Session S_1 is completed.

g. At the session S_2 the attacker sets $r_b’ = x(r_sT_{a,1})s_b$ and computes $T’_{b,1} = r_b’P$ and $T_{b,2} = [r_b’ + x(r_s’T_{a,1})s_a)Y$
h. $T’_{b,1}$ and $T_{b,2}$ is forwarded to reader.
i. When reader sends this value to the tag A, the attacker uses $T_{a,2}$. $T_{a,2}$ is calculated at the session S_1 by tag A
j. $T_{a,2}$ is forwarded to the reader
k. The reader hands down these proofs to the verifier.

Verifier calculates,
$S_aP = (y^{-1}T_{a,2} – T_{a,1})[x(T_{b,2})]^{-1}$
$S_bP = (y^{-1}T_{b,2} – T_{b,1})[x(r_s’T_{a,1})]^{-1}$
The verifier accepts the public key of attacker, because it is the public key of tag A. Now the time stamp is added.

III. PROPOSED WORK

A. Novel Secure Grouping Proof Protocol without Compromised Tag Attack (CTA)

This extended protocol solves the weakness of the ECC based RFID authentication protocol. New scheme is shown in Fig.3.

a. The reader sends “start left” to tag A. Tag A selects the random value $r_a \in_R$ Z and calculates $T_{a,1}=r_aP$. This $T_{a,1}$ value is forwarded to the reader.
b. The reader sends “start right” and $T_{a,1}$ to tag B.
c. Now tag B selects the random value $r_b \in_R$ Z and calculates $T_{b,1}$. This value is forwarded to the reader.
d. The reader selects the random value $r_s \in_R$ Z and forwards it to tag B
e. Tag B computes $T_{b,2} = [r_b + x(r_sT_{a,1})s_a]Y$ using its private key s_a and r_s and forwards it to tag A through reader.
f. Now the tag A computes the $T_{a,2} = [r_a + x(T_{b,2})s_b]Y$ and forwards this reader
g. The reader hands down these proofs to the verifier.

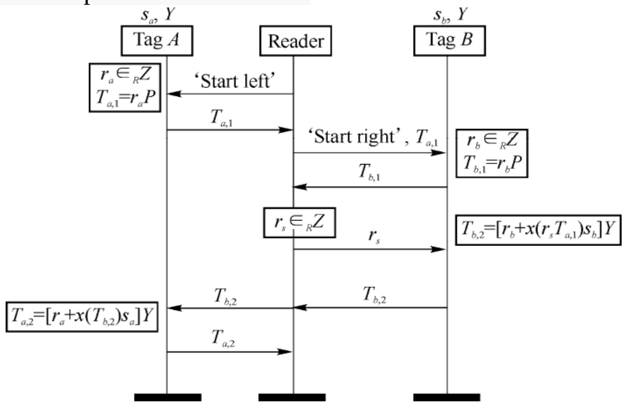

Fig. 3 Secure Grouping Proof Protocol without Compromised Tag Attack

Verifier calculates,
$S_aP = (y^{-1}T_{a,2} – T_{a,1})[x(T_{b,2})]^{-1}$
$S_bP = (y^{-1}T_{b,2} – T_{b,1})[x(r_sT_{a,1})]^{-1}$
Now the verifier verifies these public key, to check whether they have registered in database.

B. **Three Party Grouping Proof**

In which, we are using three tags such as, tag A, tag B and tag C. Tag B sends the $T_{b,2}$ to tag C instead of sending to tag A. Upon receipt of $T_{b,2}$ the tag C selects $r_c \in_R$ Z. Also calculates $T_{c,1} = r_cP$ and $T_{c,2} = [r_c + x(T_{b,2})s_c]Y$. Then forwards these $T_{c,1}$ and $T_{c,2}$ to reader. Now the reader forwards $T_{c,2}$ to tag A. Using this value tag A calculates $T_{a,2} = [r_a + x(T_{c,2})s_b]Y$. Finally the proofs of tag A, B and C are forwarded to verifier.
Verifier calculates,
$S_aP = (y^{-1}T_{a,2} – T_{a,1})[x(T_{c,2})]^{-1}$
$S_bP = (y^{-1}T_{b,2} – T_{b,1})[x(r'_2T_{a,1})]^{-1}$
$S_cP = (y^{-1}T_{c,2} – T_{c,1})[x(T_{b,2})]^{-1}$
Now the verifier checks whether these public keys are stored in database.

C. Implementation of Grouping Proof against CTA

This protocol provides the security between the tag and reader. The notation used for this implementation is listed below,

$i \in_R$ Z	The number of tags
P_i	The ith tag among all the tags
P	The base point in an elliptic curve
Y	The trusted verifier’s private key
Y(= yP)	The trusted verifier’s public key
T	The point on the elliptic curve
X(T)	The x-coordinate of the point T
S_i	The ith tag’s private key
$S_i(= s_iP)$	The ith tag’s public key

The implementation grouping proof as follows,

a. When i = 1, the reader sends “start left” to tag P_i. P_i selects random $r_i \in_R$ Z and computes $T_{i,1} = r_iP$, then forwards this to reader.

b. When i = 2, the reader forwards $T_{i-1,1}$ to tag P_i. Upon receipt of $T_{i-1,1}$ tag P_i selects $r_i \epsilon_R$ Z and computes $T_{i,1}$, then forwards this to reader. Now the reader selects random value $r_s \epsilon_R$ Z and forwards to tag P_i.Tag P_i calculates $T_{i,2} = [r_i + x(r_sT_{i-1,1})s_i]Y$ using its private key s_i and forwards this to tag P_{i+1}

c. When i = 3, tag Pi selects the random value $r_i \epsilon_R$ Z. Tag P_i computes $T_{i,1}$ and $T_{i,2}$, then forwards this tag P_{i+1}.

d. When i = n, tag P_i selects the random value $r_i \epsilon_R$ Z. Tag P_i computes $T_{i,1} = r_iP$ and $T_{i,2} = [r_i + x(T_{i-1,2})s_{i-1}]Y$, then forwards $T_{i,2}$ to reader. Reader forwards this to P_{n-i+1}. Now P_{n-i+1} calculates $T_{n-i+1,\ 2} = [r_{n-i+1} + x(T_{i,2})s_{n-i+1}]Y$ using its own private key s_{n-i+1}, then forwards this to reader.

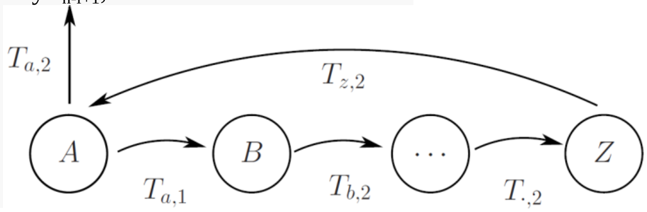

Fig. 4 Implementation of Grouping Proof against CTA

The reader forwards these proofs to verifier. The verifier verifies the proofs by using the calculation,
$s_1P = (y^{-1}T_{1,2} – T_{1,1})[x(T_{i,2})]^{-1}$
$s_2P = (y^{-1}T_{2,2} – T_{2,1})[x(T_{1,1})]^{-1}$
$s_iP = (y^{-1}T_{i,2} – T_{i,1})[x(T_{i-1,2})]^{-1}$
Where, i = 3, 4, 5 ....n
The verifier verifies the public key of the tags with registered public key in verifier database.

IV. RESULT AND PERFORMANCE ANALYSIS

Now we compare the proposed system with the three schemes (Batina, SOTP and SMGOTP).

	RA	DoS	MIM	CT
Batina	Y	Y	Y	N
SOTP	Y	Y	N	N
SMGOTP	Y	Y	N	N
Our Work	Y	Y	Y	Y

RA – Replay Attack
Dos – Denial of Service
MiM - Man-in-Middle Attack
CT – Compromised Tag Attack
Next we analyze the tag computation cost, reader computation cost and communication cost of our protocol while transferring multiple tags. And compare their performance with Batina, SOTP and SMGOTP protocols.

A. Comparison of Computation Load on Reader's Part

Fig.5 shows the comparison among the four protocols. From this figure, our protocol has the lower reader computational cost than SOTP and SMGOTP protocols. Because during the whole protocol needs one random value for all tags. But Batina work has the same computational cost as our work. The computational cost of the four protocols are given below,

Scheme	Reader Computational Cost
Batina	T_{ran}
SOTP	$3nT_{en}$
SMGOTP	$(n + 1)\ T_{en} + T_{ran}$
Our Work	T_{ran}

T_{ran} - Time taken for choosing random value

T_{en} - Time taken encryption or decryption

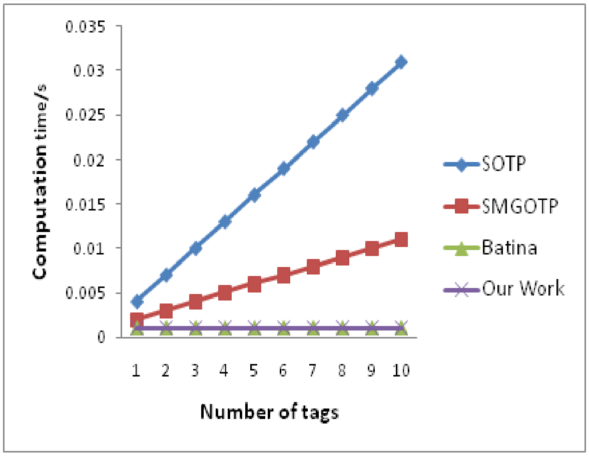

Fig. 5 Comparison of Computation Load on Reader's Part

B. **Comparison of Computation Load on Tag's Part**

Fig.6 shows the comparison among the four protocols, SOTP, SMGOTP, Batina and our work. From this figure, our protocol has the higher tag computational cost than SOTP and SMGOTP protocols. Also Batina work also has the higher tag computation cost than SOTP and SMGOTP. The reason for higher computation cost is our work and Batina protocol needs elliptic curve algorithm. But SOTP and SMGOTP uses three lightweight encryption algorithms. Although our work has higher computational cost, it has higher security. Computational cost of the four protocols are given below,

Scheme	Reader Computational Cost
Batina	$nT_{ran} + (2n + 1)\ T_{ecc}$
SOTP	$3nT_{lw} + 2nT_{ran}$
SMGOTP	$5nT_{lw}$
Our Work	$nT_{ran} + (2n + 1)\ T_{ecc}$

T_{ecc} - Time taken for elliptic curve operation
T_{lw} - Time taken for lightweight encryption or decryption
T_{en} - Time taken encryption or decryption

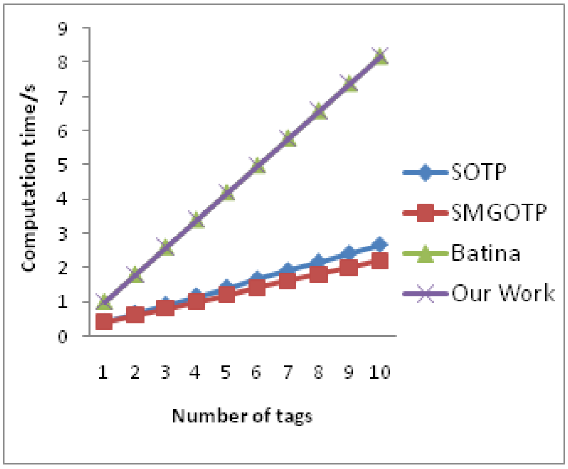

Fig. 6 Comparison of Computation Load on Tag's Part

C. Comparison of Communication Load on Tag's Part

Fig.7 shows the comparison of communication cost of the four protocols. From this figure, our protocol has the lower tag communication cost than SOTP and SMGOTP protocols. But slightly Batina work has the lower communication cost than our work. The communication cost of the four protocols are given below,

Scheme	Reader Computational Cost
Batina	N + 4
SOTP	11n
SMGOTP	2n + 7
Our Work	N + 6

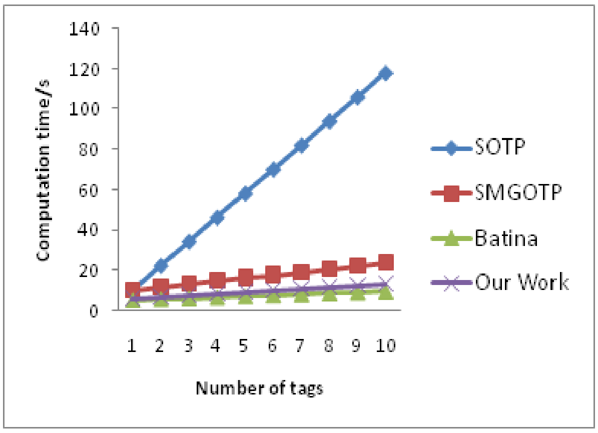

Fig. 7 Comparison of Communication Load on Tag's Part

V. CONCLUSION

There is a lot of RFID authentication protocols exists for scanning multiple tags simultaneously. They give different levels of security. Mostly these protocols concentrate on the man-in-middle attack. But they not yet concentrated on compromised tag attack. Our work overcomes compromised tag attack with man-in-middle attack. In this article, we prove that our scheme has the higher security than other three protocols Batina, SOTP and SGMOTP. Also prove that our scheme has the lower reader computation cost and communication cost than these three schemes. Although our scheme has higher tags computation cost than Batina, SOTP and SGMOTP scheme, it is still acceptable. Because it has higher security than other three protocols when transferring multiple tags.

REFERENCES

[1] Batina L, Lee Y, Seys S, et al., "Extending ECC-based RFID authentication protocols to privacy-preserving multi-party grouping proofs", Personal and Ubiquitous Computing, 16(3): 323-335, 2012.

[2] Gul N. Khan, Jack Yu and Fei Yuan, "XTEA based Secure Authentication Protocol for RFID Systems. Ryerson University", ICCCN Workshops, Vol. 24, No. 2, 381-394, February 2011.

[3] Peris-Lopez P, Orfila A, Hernandez-Castro J, et al. "Flaws on RFID grouping-proofs", Journal of Network and Computer Applications, 34(3): 833-845, 2011.

[4] Park C, Hur J, Hwang S, et al, "Authenticated public key broadcast encryption scheme secure against insiders", Journal of Mathematical and Computer Modeling, 55(1/2): 113-122, 2012.

[5] Ma C, Lin J, Wang Y, et al., "Offline RFID grouping proofs with trusted timestamps", Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'12), 674-681, Jun 25-27, 2012.

[6] Sato Y, Mitsugi J, Nakamura O, et al., "Theory and performance evaluation of group coding of RFID tags", IEEE Transactions on Automation Science and Engineering, 9(3): 458-466, 2012.

[7] Yang M H, "Secure multiple group ownership transfer protocol for mobile RFID", Electronic Commerce Research and Applications, 11(4): 361-373, 2012.

[8] Yang M H, Hu H Y, "Protocol for ownership transfer across authorities: with the ability to assign transfer target", Journal of Security and Communication Networks, 5(2): 164-177, 2012.

[9] Samad Rostampour, Mojtaba Eslamnezhad Namin, Mehdi Hosseinzadeh, "A Novel Mutual RFID Authentication Protocol with Low Complexity and High Security", I.J. Modern Education and Computer Science, 1, 17-24, 2014.

[10] Evangelos Rekleitis, Panagiotis Rizomiliotis, and Stefanos Gritzalis, “A holistic approach to RFID security and privacy”, University of the Aegean, pp. 34:1–34, 2008.

[11] Yalin Chen, Jue-Sam Chou, Chi-Fong Lin, Cheng-Lun Wu, “A Novel RFID Authentication Protocol based on Elliptic Curve Cryptosystem”, National Tsing Hua University, Volume 31, Issue 4, 648-652, June 2009.

[12] Burmester M, Medeiros B, Motta R, “Provably secure grouping-proofs for RFID tags”, Proceeding of the 8th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications (CARDIS’08), London, UK. Berlin, Germany: Springer-Verlag, 2008: 176-190, Sep 8-11, 2008.

[13] Canard, S., Coisel, I., Etrog, J., Girault, M., “Privacy-preserving RFID systems: Model and constructions”, IACR Cryptology ePrint Archive, vol. 13, no. 3, 1-13, 2010.

[14] Batina, L., Seys, S., Singel_ee, D., Verbauwhede, I. “Hierarchical ecc-based RFID authentication protocol”, In: In Proc. of CRYPTO’05, IACR, volume 3126 of LNCS, 293–308, 2011.

[15] Yi-Pin Liao, Chih-Ming Hsiao, “A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol”, Proc. of the 19th International Conference on Advanced Information Networking and Applications Volume 18, 133–146, July 2014.