International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 10, October 2016)

Cryptanalysis of Authentication Protocol Based on Low Cost Smart Card and Biometrics

El-Sayed Ahmed Ramadan[1], Mohamed Amr Mokhtar[2], El-Sayed Abdel-Moety El-Badawy[3], and Hossam Abd-Elatif Selim[4].

[1]Ph.D. Student, [2] Associate Professor, and [3]Professor,
Alexandria University, Faculty of Engineering,
Electrical Engineering Department (Communication & Electronics Section), Alexandria, Egypt.
[4]Associate Professor, Arab Academy for Science and Technology & Maritime Transport, Alexandria, Egypt,
Faculty of Engineering and Technology, Computer Engineering Department.

***Abstract*—In 2015, Odelu, Kumar and Goswami proposed a robust and efficient multi-server authentication scheme using biometrics-based smart card and elliptic curve cryptography (ECC) and claimed that their scheme could overcome all of security issues in He and Wang's scheme, such as a known session specific temporary information attack, impersonation attack, smart card loss attack, denial of service attack and perfect forward secrecy. However, it is found that Odelu, Kumar and Goswami's scheme is still insecure. In this paper, we demonstrate that their scheme is vulnerable to five types of attack as follows, replay attack, RC spoofing attack, smart card stolen attack, master key change problem and scalability problem.**

***Keywords*—Biometric Authentication Protocol, *Biometric (Fingerprint)*, Smart Card, RFID, Arduino Device, Raspberry Pi-2 Device.**

I. INTRODUCTION

Radio frequency identification (RFID) is a form of wireless communication that uses radio waves to identify and track objects. RFID technology has the capability to both greatly enhance and protect the lives of consumers, and also revolutionize the way companies do business. As the most flexible auto-identification technology, RFID can be used to track and monitor the physical world automatically and with accuracy. RFID technology connects billions of everyday items to the internet, enabling businesses and consumers to identify, locate, authenticate and engage each item. An RFID system, as shown in Figure 1[2], has readers and tags that communicate with each other by radio. RFID tags are so small and require so little power that they don't even need a battery to store information and exchange data with readers. This makes it easy and cheap to apply tags to all kinds of things that people would like to identify or track. RFID system needs server connected to the Point of Sale (POS) which has computation and storage capability to store millions of user data for authentication and identification.

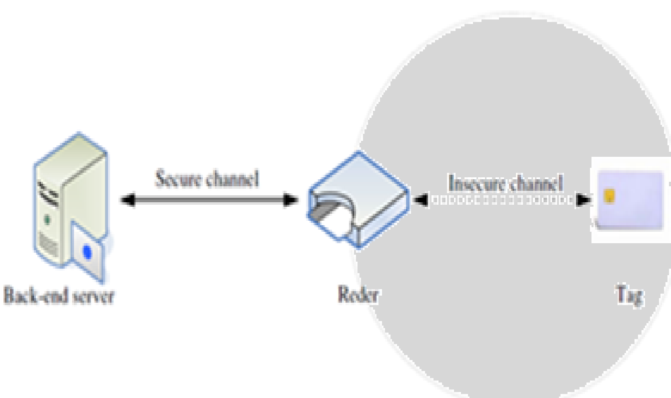


Figure1: The RFID system of the proposed scheme[2].

Many RFID authentication protocoles were introduced to protect the private data on tag. This data could value data as in transport application or personal data as in access control or access servise from web. These protocol could be classified according to as single round design[1] or multiround systems [2]. Another classification is proposed on the resources demanded by the protocols[13]. other classification is based on the kind of cryptographic approch such as public key cryptography[13]. Last classification is based on biometric authentication as shown in table 1[34] it is summerized the literature survey according to the above classification and showing the disadvantge of each system.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 10, October 2016)

TABLE I : ROUND CLASSIFICATION [34].

Paper	Approch	Disadvantages of protocol
[4]	Symmetric key or public key computations.	Not sutable for practical applications and there are high cost RFID tags.
[5]	Hash function.	Tag to be tracked.
[6]	Hash function.	Replay attack and the impersonation attack.
[7]	XOR operation, and matrix operation.	DOS attack, replay attack and individual tracing.
[8]	Hash function.	Impersonation attack and backward trace ability.
[9]	Bitwise operations.	Traceable.
[10]	Server share the tag's EPC code.	DOS attack, disguise of tags, and forward secrecy.
[11]	Simple bitwise operations.	De-synchronization attack and the fully disclosure attack.
[12]	Simple bitwise operations.	De-synchronize attack and DOS attack.
[13]	Simple bitwise operations.	De-synchronization attack and the fully disclosure attack.
[14]	Each tag has a static ID, pre-shares a pseudonym (IDS) and 2 keys with the server.	De-synchronization attack and the denial of service (DoS) attack.
[15]	Random q.k binary matrix , a random k bit vector x.	Anonymity and forward secrecy property.
[16]	Quadratic residue.	Not practical since a very large number will be used to get reasonable security level.
[17]	Quadratic residue.	
[18]	Quadratic residue.	
[19]	ECC.	Could withstand various attacks.
[20]	ECC.	
[21]	Quadratic residue.	Not suitable for practical.
[22]	ECC.	Tracking attack and the forgery attack.
[23]	ECC.	Could withstand various attacks.
[24]	Biometric-based.	Stolen smart card attack and impersonation attack.
[25]	Biometric-based.	Stolen smart card attack and impersonation attack.
[26]	Biometric-based.	Outsider attack, smart card stolen attack, impersonation attack and replay attack.[27]
[28]	Biometric-based.	Smart card loss attack and forward secrecy.[29]
[30]	Biometric based.	a known session specific temporary information attack and impersonation attack. [31]

The rest of this paper is organized as follows section 2 review of Odelu,Kumar and Goswami's Scheme, section 3 security analysis of Odelu,Kumar and Goswami's scheme finally, conclusion and future work is given in section 4.

II. REVIEW OF ODELU, KUMAR AND GOSWAMI'S SCHEME

This section reviews the biometric-based multi-server authentication scheme proposed by Odelu, Kumar and Goswami's [31]. Odelu, Kumar and Goswami's's scheme consists of six phases namely, initialization phase, registration phase, login phase, authentication and key agreement phase, password change phase, and revocation and re-registration phase.
Table II shows the notation used in this paper.

TABLE III: NOTATION Used in This Paper [34], [31].

Symbol	Description
RC	The registration center
k	The master secret key of RC
n, p	Two sufficiently large prime number
F_P	A finite field of order p
E_p	A non-singular elliptic curve over a field $GF(p)$
G	The additive group consisting of points on E_p
P	A generator of G with order n
$Ppub$	The public key of RC, where $P_{pub} = kP$
S_j	The j^{th} server
SID_j	Identity of server S_j
k_j	Private key of S_j
U_i	The i^{th} user
ID_i and pw_i	Identity and password of Ui, respectively
k_i	Authentication parameter (secret token) of Ui
SC_i	Smart card of the user Ui
Ω	Symmetric-key cryptography
$E_k(.) / D_k(.)$	Symmetric encryption/decryption using the key k
$H(.)$	A cryptographic hash function
$M_1 \backslash\backslash M_2$	Data M_1 concatenates with data M_2
$M_1 \oplus M_2$	XOR operation of M_1 and M_2
$X \rightarrow Y : (M)$	X *sends message M to* Y
$\Vert$	The concatenation operation

A. Initialization Phase

In this phase, the registration centre RC declares its public parameters $\{p, E_p, P, P_{pub}, n, H(\cdot), \Omega\}$.

B. Registration Phase

1) User Registration Phase:

$$k_i = H(ID_i \Vert k \Vert r_i)$$

$$z_i = k_i \oplus H(pw_i \Vert \sigma_i)$$

$$S_i = H(k_i \Vert I D_i \Vert H(pw_i \Vert \sigma_i))$$

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 10, October 2016)

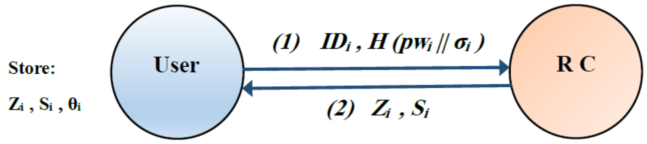


Figure2: User Registration [34].

2) Server Registration Phase:

$K_j = H(SID_j \,||k||r_j)$
$S_j = H(k \,||r_i \,||k_i \,||SID_j))$

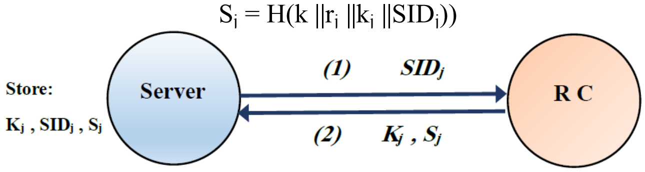


Figure3: Server Registration [34].

C. Login , Authentication and Key Establishment Phase

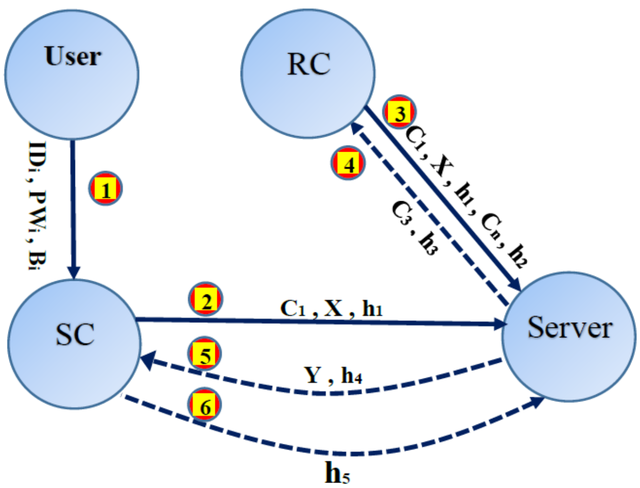


Figure4: Login, Authentication and Key Estaclishment [34].

In order to login to a server S_j, the user U_i needs to execute the following steps as in figure 4.

Step 1:

U_i inserts his/her smart card SC_i into a card reader and inputs pw_i, ID_i and imprints the personal biometrics B_i at the sensor. Then, SC_i computes $\sigma_i = Rep(B_i,\theta_i)$ and $k_i = z_i \oplus H(pw_i||\sigma_i)$ and checks whether $H(k_i||ID_i||H(pwi||\sigma_i))$ matches with si stored in the smart card SC_i.

Step 2:

$X = xP$, $K_1 = xP_{pub}$ using $x = H(x_i||k_i||n_1)$
$C_1 = E_{K1}\,(ID_i\,, SID_j\,, S_j\,, n_1)$
$X = H\,(X_i \,||\, K_i \,||\, n1)\,P$
$h_1 = H\,(\,ID_i \,||\, SID_j \,||\, S_j \,||\, n_1 \,||\, K_i \,||\, X \,||\, K_1)$

Step 3: $C_2 = E_{H(Kj\,||h1)}\,[n_1]$
$h_2 = H\,(C_1|| \,X \,||\, h_1 \,||\, SID_j \,||\, K_j \,||\, S_j \,||\, n_2)$

Step 4:

- RC computes $K_2 = kX(= K_1)$ and obtains ID_i, SID_j, S_j, and n_1 by decrypting C_1 using K_2.
- RC checks the freshness of n_1, and also checks validity of SID_j and ID_i by checking $H(SID_j||k)$ and $H(ID_i||k)$, respectively, in T.
- RC retrieves rj and ri corresponding to SID_j and ID_i, respectively, from T.
- RC computes $k_i = H(ID_i||k||r_i||H(ID_i||k))$ and $k_j = H(SID_j||k||r_j)$
- checks the conditions h_1 and S_j hold or not.
- RC computes $n_2 = D_{\,H(kj||h1)}(C_2)$ and authenticates the server S_j by checking the condition h_2.
- RC computes
    - $K_{i,j} = H(k_i||K2||n_1)$
    - $C_3 = E_{H(kj\,||\,h1||\,n2)}\,[SID_j \,||\, k_{i,j}]$
    - $h_3 = H(k_j \,||h_2||C_3||SID_j||k_{i,j}||X||n_2)$

Step 5:

- Check h_3.
- S_j confirms that the secrets $k_{i,j} = H(k_i||K_2||n_1)$ and X are shared by the legal user U_i, and $k_{i,j}$ is only known to RC, U_i and S_j.
- Then, S_j compute
    - $Y = y\,P$
    - $SK = H(yX \,||\, K_{i,j} \,||\, S_j)$
    - $h_4 = H\,(SID_j \,||\, S_j \,||\, h_1 \,||\, K_{i,j} \,||\, X \,||\, Y \,||\, SK)$

Step 6:

- Checks h_4
- U_i authenticates S_j as the hash value $k_{i,j}$ is only known to RC, U_i and S_j.
- U_i then computes $h_5 = H(SID_j||k_{i,j}||X||Y||SK)$

Finally:

S_j checks whether the condition h_5 holds or not. If it holds, both user U_i and server S_j agree on the common session key SK.

D. Password Change Phase

In this phase, U_i can change his/her password pw_i without further contacting the RC using the following steps:

Step 1:

- Inputs pw_i, ID_i and imprints personal biometrics B_i.
- SC_i computes $\sigma_i = Rep(B_i,\theta_i)$ and $k_i = z_i \oplus H(pw_i||\sigma_i)$
- Checks the condition $s_i = H(k_i||ID_i||H(pw_i||\sigma_i))$.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 10, October 2016)

Step 2:

Ui enters his/her chosen new password, say pw^{new} into the smart card SC_i.

Step 3:

SC_i computes $z^{new} = k_i \oplus H(pw^{new} \| \sigma_i)$ and $s^{new} = H(k_i \| ID_i \| H(pw^{new} \| \sigma_i))$.

Step 4:

SC_i replaces z_i and s_i with z^{new} and s^{new}.

E. Revocation and Re-Registration Phase

In this phase, we explain the user revocation and re-registration with the same identity when his/her authentication key is compromised or the smart-card is lost/stolen.

- RC verifies his/her personal identities.
- Removes the random number r_i from the table T.

Re-registration of U_i with the same identity steps:

- RC verifies T whether the identity ID_i is valid, that is, whether the user U_i is already registered, but the status is inactive. If it is valid,
- RC executes the registration phase to reactivate U_i's account.

III. SECURITY ANALYSIS OF ODELU, KUMAR AND GOSWAMI'S SCHEME

In this section, we demonstrate the vulnerability of Odelu, Kumar and Goswami's's scheme in various communication scenarios.

A. Replay Attack

An outsider adversary U_a eavesdrop a communication between a user and the server and then may try to use these messages for opening a communication to a server in future. An adversary U_a may eavesdrop a communication and store the login messages, $\{C_1, h_1, X\}$, and keep it for certain time until another login from the legal user happen to change the nonce value in verifier table. The following steps show the attacks:

- U_a send delayed message $\{C_1, h_1, X\}$ to server S_j.
- Server S_j will accept message and generate message $\{C_1, h_1, X, C_2, h_2\}$ and send to RC via a public channel. (The server could not detect the freshness of message or the identity of the user)
- RC decrypt C_1 and obtains ID_i, SID_j, S_j, and n_1
- RC checks the freshness of n_1, and also checks validity of SID_j and ID_i in table T.
- RC will accept message because RC keeps only last value of n_1 and could not detect it replayed message.
- RC will update the status field in table T to 1, which means the user is active and logged on.
- RC computes $k_{i,j}$, C_3, h_3 and send to server via a public channel.
- Server will terminate the session because the adversary U_a cannot compute the valid h_5.
- Neither the user nor server could change the status field in RC. And consequently RC will reject any login in future (the author use status field to prevent many login and use it in revocation phase).

B. RC Spoofing Attack

Assume untrusted RC and the attacker gets information about verifier table and master key k.

In this case the spoofing attack will be able to control all users during authentication phase as follows:

1) After receiving the message M2 from S_j, RC computes $K_2 = kX(= K_1)$ and obtains IDi, SID_j ,s_j, and n_1 by decrypting C_1 using K_2.

2) RC checks $H(SID_j \| k)$ and $H(ID_i \| k)$, respectively, and retrieves r_j and r_i.

3) RC computes $k_i = H(IDi \| k \| r_i \| H(ID_i \| k))$ and $k_j = H(SID_j \| k \| r_j)$.

4) RC computes $k_{i,j} = H(ki \| K_2 \| n_1)$, $C_3 = E_{H(kj \| h1 \| n2)}[SID_j \| k_{i,j}]$ and $h_3 = H(k_j \| h_2 \| C_3 \| SID_j \| k_{i,j} \| X \| n_2)$.

Finally, RC sends the message $M_3 = \{C_3, h_3\}$ to Sj via a public channel.

C. Smart Card Stolen & Off-line Identity Guessing Attack

Smart card stolen attack means an adversary who possessed with smart card performs any operation which the smart card and obtains any information. If an outsider adversary U_a steals the smart card of legitimate user U_i and obtains parameters Public sketch θ_i, z_i and S_i.

The public sketch θ_i and σ_i is obtained using fuzzy extractor [32]. A fuzzy extractor has two disadvantages.

- The public sketch θ and the authentication key σ are extracted from the biometric and cannot be renewed.
- it has been shown that it is impossible [33] to build fuzzy extractors for which the output does not leak information about the biometric input and then we can obtain σ_i

The attacker could apply offline Identity Guessing attack on the following equation:

$S_i = H(z_i \oplus H(pw_i \| \sigma_i) \| ID_i \| H(pw_i \| \sigma_i))$

Where ID_i is 32 bit and consequently could obtain user key

$k_i = z_i \oplus H(pw_i \| \sigma_i)$

D. Master Key Change Problem

In registration phase the unique mater key is involved to create the following:

1) Identity of each register user by calculating $H(ID_i \| k)$

2)generation of user key by calculating $H(ID_i \| k \| r_i)$

The proposed schema will fail to update master key because it is shared for all register user. The procedure for changing this key will need to re-registration for all users once again.

E. Scalability Problem

The server should be able to handle growing amounts of work in a large tag population. Performing an exhaustive search to identify individual tags could be difficult when the tag population is large. Another operational requirement is the uniqueness of Meta-IDs. One problem is that we cannot assure the uniqueness of hash outputs. In order to avoid the conflictions of hash outputs, we need to have enough length of hash outputs. Otherwise the confliction of Meta-IDs can cause serious problems in the system. In another word, if we can make sure the uniqueness of Meta-IDs, we can reduce the size of Meta-IDs, which means the reduction of transmission and memory.

IV. CONCLUSION

In 2015, Odelu, Kumar and Goswami's's proposed an enhanced scheme of He and Wang's scheme and demonstrated it is resistances to famous attacks such as impersonation attacks, smart card stolen attacks, off-line password guessing attacks, man-in-the middle attacks and replay attacks. However, Odelu, Kumar and Goswami's's scheme is still insecure. In this paper showed how their scheme can suffer to five types of attack as follows, replay attack, RC spoofing attack, smart card stolen attack, master key change Problem and limited scalability problem.

Finally, in this paper further research direction ought to propose a secure user authentication scheme. Which we can solve these problems in the future work a proposed solution will be introduced.

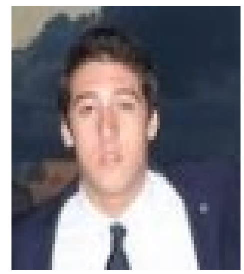
ACKNOWLEDGEMENT

The authors would like to thank

Mr. Ahmed Hossam,

Student at Arab Academy for Science and Technology & Maritime Transport,

Faculty of Engineering & Technology, Computer Engineering Department, Alexandria, Egypt, for his valuable help in trouble shooting and devices programing.



References

[1] S. Piramuthu, “Protocols for RFID tag/reader authentication”, Decision Support Systems 43(3), pp. 897-914, 2007.

[2] Zhenguo Zhao " A Secure RFID Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptosystem"J Med Syst (2014) 38:46 - Received: 6 February 2014 /Accepted: 20 March 2014 /Published online: 23 April 2014

Springer Science+Business Media New York 2014.

[3] Hung-Yu Chien "The Study of RFID Authentication Protocols and Security of Some Popular RFID Tags"
Source: Development and Implementation of RFID Technology, Book edited by: Cristina TURCU,
ISBN 978-3-902613-54-7, pp. 554, February 2009, I-Tech, Vienna, Austria.

[4] A. Juels, R. Rivest, and M. Szydlo, “The Blocker Tag: Selective Blocking of RFID tags for Consumer Privacy,” 8th ACM Conf. Computer and Comm. Security, V. Atluri, ed., ACM Press, 2003, pp. 103–111.

[5] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems,” In the Proceedings of the First Security in Pervasive Computing, LNCS, Vol. 2802, pp.201-212, 2003.

[6] M. Ohkubo, K. Suzuki, and S. Kinoshita, “Cryptographic approach to ‘Privacy-friendly’tag,” in RFID Privacy workshop, MIT, USA, 2003.

[7] S. Karthikeyan, M. Nesterenko (2005), “RFID security without extensive cryptography,”Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pp. 63-67.

[8] Henrici, D., and Muller, P., Hash based enhancement of location privacy for radio frequency identification devices using varying identifiers. International Workshop on Pervasive Computing and Communication Security—PerSec 2004, IEEE Computer Society, 149–153, 2004.

[9] Lim, C., and Kwon, T., Strong and robust rfid authentication enabling perfect ownership transfer. Information and Communications Security, Lecture Notes in Computer Science, Springer, 4307:1–20, 2006.

[10] D. N. Duc, J. Park, H. Lee and K. Kim (2006), "Enhancing Security of EPC global Gen-2 RFID Tag against Traceability and Cloning," The 2006 Symposium on Cryptography and Information Security.

[11] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez- Tapiador, and A. Ribagorda, "EMAP: An Efficient Mutual Authentication Protocol for Low-cost RFID Tags," in: OTM Federated Conferences and Workshop: IS Workshop, November 2006.

[12] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFIDtags", in: Proc. of 2nd Workshop on RFID Security, July 2006.

[13] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda,"M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags", in: Proc. of International Conference on Ubiquitous Intelligence and Computing UIC'06, LNCS 4159, pp. 912-923,Springer,2006.

[14] H. Y. Chien, "SASI: A New Ultra-Lightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity," IEEE Transactions on Dependable and Secure Computing 4(4), October, 2007.

[15] A. Juels and S. Weis. Authenticating Pervasive Devices with Human Protocols. Adv. In Cryptology | Crypto 2005, LNCS vol. 3621, Springer-Verlag, pp. 293-308, 2005.

[16] Chen, Y., Chou, J. S., and Sun, H. M., A novel mutual authentication scheme based on quadratic residues for RFID systems. Comput. Netw. 52(12):2373–2380, 2008.

[17] Yeh, T. C., Wu, C. H., and Tseng, Y. M., Improvement of the RFID authentication scheme based on quadratic residues. Comput.Commun. 34(3):337–341, 2011.

[18] Doss, R., Sundaresan, S., and Zhou, W., A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems. Ad Hoc Netw. 11(1):383–396, 2013.

[19] Tuyls, P., and Batina, L., RFID-tags for anti-counterfeiting. Lect. Notes Comput. Sci 3860:115–131, 2006.

[20] Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., and Verbauwhede, I., Public-key cryptography for RFID-tags. In: Fifth IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 217–222, 2007.

[21] Lee,Y.K., Batina, L., andVerbauwhede, I., EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID Authentication Protocol, IEEE International Conference on RFID, pp. 97–104, 2008.

[22] Bringer, J., Chabanne, H., and Icart, T., Cryptanalysis of EC-RAC, a RFID identification protocol. In: International Conference on Cryptology and Network Security—CANS'08, Lecture Notes in Computer Science: Springer-Verlag, 2008.

[23] Liao, Y. P., and Hsiao, C. M., A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Networks, 2013.doi:10.1016/j.adhoc .2013.02.004.

[24] M.C. Chuang and M.C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," Expert Systems with Applications, Vol. 41, No. 4, pp. 1411-1418, 2014.

[25] D. Mishra, A. Das and S. Mukhopadhyay, "A secure user anonymity preserving biometric-based multi-server authenticated key agreement scheme using smart cards," in Expert Systems with Applications, vol.41, pp. 8129-8143, 2014

[26] K. Baruah, S. Banerjee, M. Dutta and C. Bhunia,"An Improved Biometric-based Multi-server Authentication Scheme Using Smart Card," in International Journal of Security and Its Applications, vol.9, pp. 397-408, 2015.

[27] Jongho Mun, Jiye Kim, Donghoon Lee and Dongho Won

"Cryptanalysis of Biometric-based Multi-server Authentication Scheme Using Smart Card" in 11th International Conference on Heterogeneous Networking for Quality, reliability, Security and Robustness (QSHINE) 2015.

[28] Y. Choi, J. Nam, D. Lee, J. Kim, J. Jung and D. Won "Security enhanced anonymous multi-server authenticated key agreement scheme using smart card and biometrics," The Scientific World Journal, Vol. 2014, Article 281305 , 2014.

[29] Wen-Chung Kuo, Hong-Ji Wei, Yu-Hui Chen, Jiin-Chiou Cheng, "An Enhanced Secure Anonymous Authentication Scheme Based on Smart Cards and Biometrics for Multi-Server Environments"IEEE 10th Asia Joint Conference on Information Security 2015.

[30] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," IEEE Syst. J., published volume 9, Issue 3, September 2015.

[31] Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami- "A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards"- IEEE Transactions on Information Forensics and Security, Vol. 10, No. 9, September 2015.

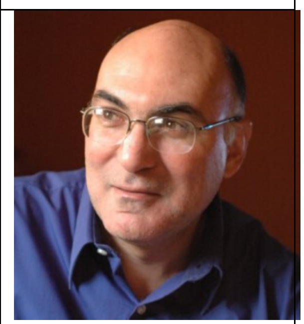
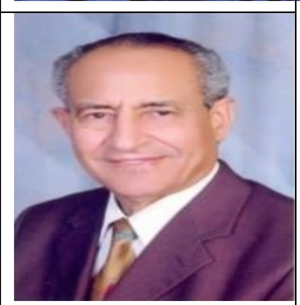
[32] [32]Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in Advances in Cryptology. Interlaken, Switzerland: Springer-Verlag, 2004, pp. 523–540.

[33] Y. Dodis and A. Smith. Correcting errors without leaking partial information. In Harold N. Gabow and Ronald Fagin, editors, Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC), Baltimore, MD, USA, May 22-24, 2005, pages 654–663. ACM, 2005.

[34] Extracted from Ph.D. thesis, El-Sayed Ahmed Ramadan, (under preparation), registered for Ph.D. In Communications and Electronics, Spring 2015, Faculty of Engineering, Alexandria University, Electrical Eng. Dept., Egypt.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 10, October 2016)

AUTHORS PROFILE:

Teaching Assistants: El-Sayed Ahmed Ramadan; Teaching Assistants, Borg Al-Arab Higher Institute of Engineering &Technology, Alexandria, Egypt. Registered for Ph.D. in Communications and Electronics, Spring 2015, Electrical Eng. Dept., Faculty of Engineering- Alexandria University, Alexandria 21544, Egypt. B.Sc. & M.Sc. in Communications and Electronics, 1994, 2014, respectively. M.Sc. thesis title: Advanced Cellular Mobile Communication Systems. Publications extracted from M.Sc. thesis: Two Journal papers. Point of Research: Security in mobile data.	
Associate Professor: Mohmed Amr Mokhtar Electrical Eng. Dept., Faculty of Engineering- Alexandria University, Alexandria 21544, Egypt. Graduated in1983 from Alexandria University with Honors, Obtained M.Sc. in 1988 in Digital Speech Processing, Got Ph.D. in Digital Mobile Communications from Southern Methodist University, Dallas, Texas 75275, USA, in 1992. His current interests are in Secure Communications, Encryption, Coding Techniques, and Digital Signal Processing.	
Prof. Dr El-Sayed Abdel-Moety El-Badawy; SM IEEE & OSA Member. Distinguished Professor Emeritus of Communications & Electronics, Electrical Eng. Dept., Faculty of Engineering- Alexandria University, Alexandria 21544, Egypt.	
Associate Professor: Hossam Abd-Elatif Selim Computer Engineering Department, Faculty of Engineering &Technology. Arab Academy for Science and Technology & Maritime Transport, Alexandria, Egypt. Ph.D. in Electronic Engineering: pursing in the field of secure document modeling using biometric technique at the Electronic Engineering Laboratory of the University of Kent, at Canterbury, UK.