

# Lightweight ECC based RFID Authentication Protocol



Sanjeev Kumar, Aditya M Pillai, Amulya Bhardwaj, Gopesh Mitta

**Abstract:** *The RFID (radio frequency identification) technology is being extensively accepted and used as a governing recognizing technology in medical management domain like information corroboration, patient records, blood transmission, etc. With more rigid security concern to RFID based authentication protocols, ECC (elliptic curve cryptography) established Radio Frequency Identification verification protocols is being expected to fit the prerequisite of security and privacy. However, abounding new published ECC based RFID protocols have severe security vulnerability. In the following paper, we have reviewed few RFID verification and authentication protocols and has compared its strengths, fragility and proposed less complex and more efficient authentication protocol.*

**Keywords:** *Lightweight Elliptical Curve Cryptography, RFID, Radio Frequency Identification, Random Cyclic Redundancy Analysis.*

## I. INTRODUCTION

The RFID (radio frequency identification) technology allows the automated, noncontact and exclusive recognition of objects using radio waves and it is studied as the finest reinstatement of the existing barcode technologies. [1] RFID technology is being accepted in an extensive diversity of corporation and being progressively used in various fields, like manufacturing, management, supply chain, inventory management, e-passport processing, etc. [2]. Inclusion to various utilization in our day to day life, the RFID is already a big part of the health care field. For example, it is being used for location tracking of medical and health capitals, in-patient and out-patient identification and validation, health treatments progress tracking, locating patients and procedure administration at the wellbeing place, and surgical management [3–6]. The main peripheral of RFID systems are back-end servers, tags and readers. RFID tag is a recognition gear affixed to object that is to be recognized, which makes use of RF (radio frequency) to connect and establish identification of item being read.

RFID reader is also a gear which can be used to observe the presence of RFID tags on any object nearby and collect the data being supplied by tag to reader. The reader identifies the tags by transmitting radio frequency signals, and tag acknowledge to the reader with a particular number or any other identifying data. The reader promotes the RFID tag response data to the back-end of the RFID device i.e. servers. The server has several databases containing tags information and its related data and is capable of retrieving complete facts and information required related to the tag from the tag response/data being fed. The main assets of RFID devices are that, it gives automated and various identification seizure and system performance analysis. RFID readers can automatically scan numerous tags at the same time, also be used to track important items. However, RFID systems makes the security and privacy of the holder of the tag vulnerable, as the result of automated verification and identification. [7] In this paper, we are providing with a RFID protocol that is based on ECC (Elliptic Curve Cryptography). We implemented the protocol in telosb using TinyOS NesC. We also implemented another existing protocol and performed a comparison between our and the existing protocol and thus it can be clearly understood that our protocol provides faster communication.

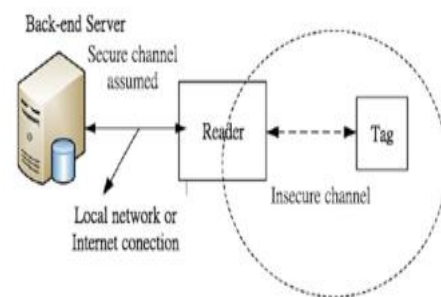


Fig. 1- A typical RFID-based system

## II. PROBLEM STATEMENT

RFID tags are lightweight and resource constraint. These components have limited amount of battery power, memory. Security issue comes in case of communication with RFID tags. Different authentication protocols have been proposed to secure the data transmission. But due to privacy security issues, all standard encryption decryption algorithms authentication protocols cannot be used. We are proposing a verification and authentication scheme in this paper. Some of the major motivation and scopes are enlisted below:

- Resource constraint components have limited amount of battery power, memory.
- Secure data transmission between lightweight devices.

Revised Manuscript Received on May 30, 2020.

\* Correspondence Author

**Aditya M. Pillai\***, Department of Computer Science and Engineering, ABES Institute of Technology, Ghaziabad, Affiliated to AKTU Lucknow, India. E-mail: vmpillai786@gmail.com

**Amulya Bhardwaj**, Department of Computer Science and Engineering, ABES Institute of Technology, Ghaziabad, Affiliated to AKTU Lucknow, India. E-mail: amulya.b520@gmail.com

**Gopesh Mittal**, Department of Computer Science and Engineering, ABES Institute of Technology, Ghaziabad, Affiliated to AKTU Lucknow, India. E-mail: gmittal877@gmail.com

**Sanjeev Kumar**, Department of Computer Science and Engineering, ABES Institute of Technology, Ghaziabad, Affiliated to AKTU Lucknow, India. E-mail: sanjeev.kumar@abesit.in

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

### III. EXISTING RFID AUTHENTICATION PROTOCOLS

There are various numbers of research papers and groups that are being burdened by the security and privacy significance of the RFID (Radio Frequency Identification) systems and its various authentication and validation protocols for the same are being designed. In the following paper, we have covered the current works regarding RFID authentication protocols. The way RFID tags and scanner work, they can be categorised into three tags: passive, active and semi active tags. Passive are the one, being used in related protocols. Juels [8] created verification and authentication scheme with the help of message authentication functions and hash code functions to construct protocols for medical applications. Making improvements in his work, Wong al. [9] too used same functions to construct “hash-lock” protocol. sadly, Chen et. [10] discovered that Juel al.’s protocol was unable to provide RFID tag anonymity and can easily fall prey to rep0lay attack by the intruder. He also stated that [10] Wong al.’s protocol was unable to provide with location secrecy along with being prone to the impersonation and the replay attack. [11].

Further to enhance RFID security and performance issues, Chien used the random cyclic redundancy analysis to construct a mutual identification and authentication protocol. With time, Lopez al. [12] discovered that protocol being developed by Chien was unable to ensure forward privacy along with location secrecy. To resolve these issues, Lo al. [13] introduced a better protocol for authentication inspired from Chien’s proposal. Nonetheless, Yeh al. [14] stated that Loal.’s [13] proposal was still not able to provide location secrecy. A new authentication protocol was introduced by Yeh et al. [14] with improved privacy and security. However, Yeh et al.’s was not able to provide security from the server impersonation and the data integrity attacks from the intruder, because of the fact that data was being transferred to server in the plain text format. Cho et al. [15] made use of the similar message authentication code functions and hash functions to create a better and secure authentication protocol.

However, Cho et al.’s scheme was very prone to the various attacks like resynchronization, the tag impersonation and the impersonating reader’s attack, which was shown by Safkhani et al. [16] in his proposal. New studies on, the public key cryptography like ECC is also used in the design of RFID identification and authentication protocols. Chen et al. in his paper was the first to propose the RFID identification and authentication protocol with the help of quadratic residues in his work. Later on, Cao and Shen [17] discovered that Chen’s proposal was very much prone to the tag impersonation attack and the replay attack. In order to resolve these security issues, Yeh and Wu [18] provided with enhanced RFID authentication protocol with the help of quadratic residues. Further, for making the system efficiency better, Doss al. [19] developed a new RFID identification and authentication protocol similarly with the quad residues.

In comparison with the cryptography using quadric residues, the *Elliptic curve cryptography (ECC)* was able to provide the equivalent level of privacy and security with much smaller key size as compared to previous approaches. Thus, ECC-based RFID identification and authentication protocol

is much more efficient. Lee et al. [20] created an ECC-RFID protocol for authentication and declared that their protocol is probably more secure and efficient. Nonetheless, Bringer and Deursen discovered that Lee’s protocol was prone to the various attacks like tracking attack and the replay attack. Now, for enhancing the privacy and security, Lee [20] created yet other RFID authentication scheme/protocol.

Nonetheless, Deursen [18] showed that Lee’s protocol [20] was still defenceless to the tracking attack. Further, a new ECC-based RFID authentication protocol was developed by Lee [17] to conquer vulnerability in various previous protocols. Sadly, later on it was indicated by Lv et al. [17] that Lee’s 3 protocols are very much prone to the tracking attack. Newly introduced work by, Liao and Hsiao gave an ECC-based RFID identification and authentication protocol unified with an ID-verifier transmission scheme and asserted that their protocol can be easily implemented to provide security from various threats. Nonetheless, further it was shown in Peeters and Hermans work [18],that Liao and Hsiao’s proposal was very much prone to the server impersonation attack.

#### A. Liao and Hsiao Authentication Protocol

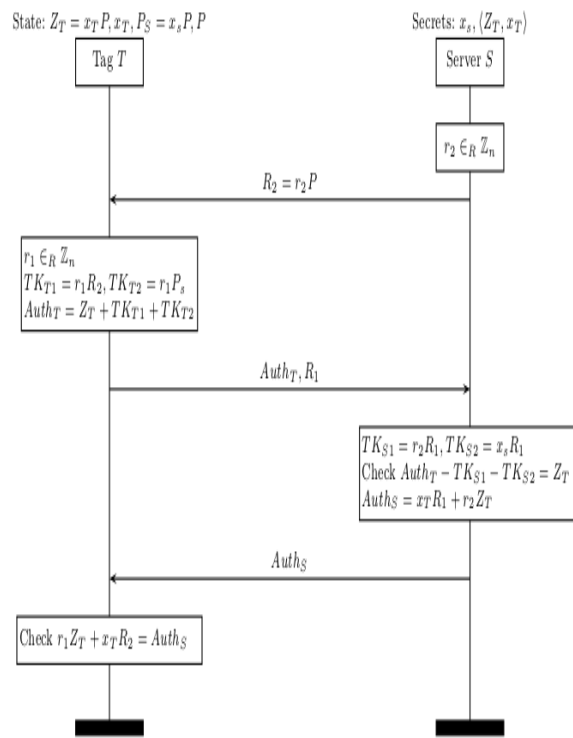
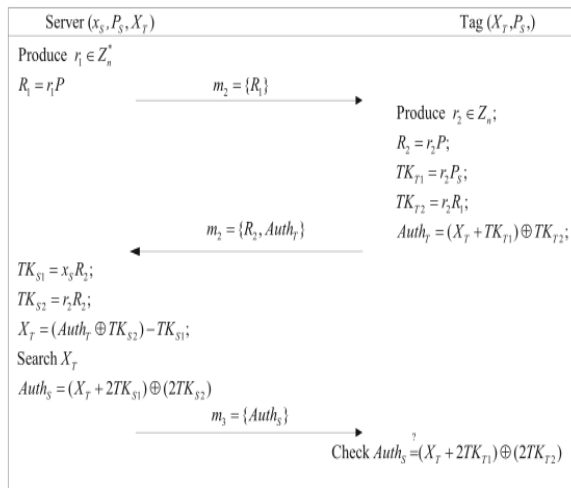


Fig. 2- Liao and Hsiao’s scheme

The writer gave their authentication rules on the basis of public key cryptanalysis but did considered the fact 1) tag-attestation is established on the transmitted privacy  $Z_T$ , and 2) Identification of the server is established on the transmitted secret data  $x_T$ . For tag-identification the public data of the tag is masked using an unauthenticated Diffie-Hellmann compliance scheme to solve  $TK_{T1} = TK_{S1}$  and an implicit authenticated variant to compute  $TK_{T2} = TK_{S2}$ . For RFID server verification of the value of  $R_1$  and  $R_2$  is crossed with the tag’s private key  $x_T$ .

**B. Debiao He's Authentication Protocol**



**Fig. 3- Debiao He's scheme**

**C. Issues in existing protocols**

Tag-authentication and secrecy depend on the lack of the attacker knowledge to know the tag's public component  $Z_T$ . Nonetheless, it freely can get the information about the tag, without physical attack, Directly by transmitting  $R_2 = -P_S$ . It refers to fact that the tag will convey to tag,  $Auth_T = Z_T - r_1P_S + r_1P_S = Z_T$ . The executive ability is to withdraw this unique identifier which enables no secrecy properties can be obtained. Here, the elemental attack prones can easily be reduced by tag analyzing that  $R_2 = -P_S$ .

Yet, the intrusion can freely be continued by approximating  $R_2 = -P_S + \alpha P$  along  $\alpha \in_R Z_N$ . Now the conclusion from the tag is given as  $Auth_T = Z_T + r_1(-P_S + \alpha P) + r_1P_S = Z_T + \alpha r_1P$ . The mugger thus now easily recover  $Z_T = Auth_T - \alpha r_1P$ . Shared privacy used in RFID helps in achieving Server-attestation. Yet, Liao and Hsiao explained in their proposal server spoofing attack as an intrusion where the attacker is apt to imitate a server to a tag whose safety is being compromised (i.e. access to the tag's secret data). Thus, the intruder gains knowledge about  $xT$  - tag and transmits  $x_T(R_1 + R_2)$ , strongly verifying as the genuine server. Here, it can be noted that there is no requirement of any data even  $r_2$  for this intrusion.

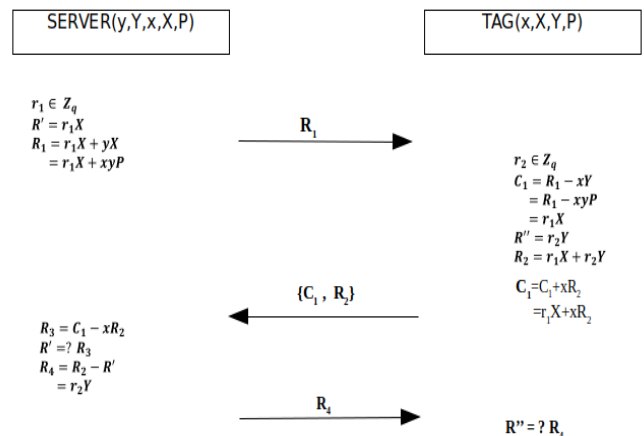
For mutual verification theorem of RFID system it can be contend that it is not that important concern for the private RFID verification scheme. Yet, if additional information is to be send by tag or sever, for instance, RFID readings, authentications are vital.

Thus both tag and server-attestation is not obtained, thus further it fails to obtain mutual authentication. Therefore, the proposed scheme by Liao and Hsiao is very much prone mainly from existing homomorphic schemes consisting the input-output data which can be easily attacked. Thus resulting into less secure and private functions is obtained by this protocol.

**IV. PROPOSED PROTOCOL**

- $F(q)$ : field size is given by  $q$  and  $F(q)$  defines the finite field.
- $a, b$ : two parameters of an elliptic curve  $E$ .
- $y^2 = x^3 + ax + b$  represents the elliptic curve  $E$ , over the limited field  $F(q)$ .
- $P$ : generator point.

- $y$ : Server's private key.
- $x$ : private key for the Tag
- $R_1, R_4$ : message from server to tag.
- $C_1, R_2$ : message from tag to server.



**Fig. 4- Proposed protocol**

- Information regarding the private and public keys of server and tag are stored in server, whereas, but no access of server's private key is given to the tag.
- $R'$  and  $R_1$  values are calculated by server.  $R_1$  is sent to the tag. When received,  $R_1$  is where tag performs an operation which results in  $C_1$ .
- $R''$  is calculated and  $R_2$ , updates  $C_1$ .  $C_1$  and  $R_2$  are sent to the server.
- The server performs operation on  $C_1$  and  $R'$  result matching is done with the former.
- If matching fails, communication is stopped, else on  $R_2$ , an operation is performed by server which results in  $R_4$  which in turn is sent to the tag.
- The tag, when received, checks are done for if values are matched with  $R''$ .
- If matching is successful then only communication is further continued, which means both sides have been successfully authenticated, else no communication will take place.

**V. ANALYSIS OF SECURITY**

**A. Theorem 1: Mutual Authentication**

No generation of legal message  $R_1$  is carried without the information of  $r_1$  and  $y$  where  $r_1$  is the randomized number that is generated by the server and  $y$  being the private key of the server. Only server knows both these values and they are not passed during the communication, this maintains the secrecy of the two values, and hence is only stored in server. No generation of legal message  $R_2$  can happen without the information of  $r_2$  and  $x$ ,  $r_2$  being a random generated number by tag and  $x$  being the tag's private key. Thus, Mutual Authentication between the tag and the server could be ingraind by the proposed scheme.

**B. Theorem 2: Anonymity**

Tag  $x$  has a secret key which is known by the tag and server both. In any step, given value never be passed in any occurring step of the process and hence cannot be fetched in any way.

Therefore, private key can never be fetched:  $x$  for the tag and our proposed protocol can exhibit anonymity.

**C. Theorem 3: Availability**

By the representation of our proposed protocol, it is clear that no synchronous update of the private key is required in protocol execution. Therefore execution of the proposed protocol can be completed among the server and the tag. Therefore, availability is provided by our proposed protocol.

**D. Theorem 4: Forward Security**

Suppose in any case secret key of tag,  $x$ , can be fetched. However, it cannot be determined if the messages  $R_1$  and  $R_2$  are being transmitted between the tag and the server since he has no idea about  $r_1$  and  $r_2$  for them being random numbers. So, tag cannot be traced and hence forward security could be exhibited by proposed protocol.

**E. Theorem 5: Replay Attack**

Inferring that the data  $R_1$  is being intercepted and replayed to tag. However,  $R_4$  cannot be generated upon receiving the message  $C_1$  and  $R$  since  $r_2$  being the new randomized number is being produced by tag and tag's private data  $x$  is not known. Thus, the tag is unable to find the attacker by checking the  $R_4$  correctness measure. Similarly, we can show how the server could find the replay attack by checking the  $R_3$  correctness measure. Therefore, replay attack can be held back by our proposed protocol.

**F. Theorem 6: Impersonation Attack**

The legal message  $C_1, R_1$  has to be generated by the attacker, to imitate the tag to the server. Though, the adversary cannot generate  $C_1$  and  $R_1$  because he does not know  $r_2$  and  $x$ . Thus, the proposed protocol can combat the impersonation attack.

**G. Theorem 7: Server Spoofing Attack**

To imitate the server to the tag, the adversary can generate a random number  $r_1$ , compute  $R'$  but he cannot generate  $R_2$  as they do not know the server's secret key  $y$ , neither they know the tag's secret key  $x$ . Hence, the attacker cannot imitate the server to the tag and the illustrated scheme can combat server spoofing attack.

**H. Theorem 8: DoS Attack**

In the given scheme, the tag's secret key  $x$  needs no concurrently update after the scheme is executed as the tag's secret key is well secured. Thus, the proposed scheme can combat DoS attack.

**I. Theorem 9: Location Tracking Attack**

Assume that the tag's secret key  $x$  can be hacked by the attacker and seize the messages. To get the server's secret key  $y$  and two random values  $r_1$  and  $r_2$ , the attacker does not have the capabilities to obtain that secret key, hence it cannot confirm that either those messages are communicated between the server and the tag. Thus, the illustrated scheme can overcome the location tracking attack.

**J. Theorem 10: Cloning Attack**

In the illustrated scheme, we know that each tag consists of their own private data  $x$ . Suppose this private data/key of various number tags can be hacked by the attacker. since, there is no correlation among tag's secret key, so that he cannot get the private data of another tag. Therefore, the proposed protocol can combat cloning attack.

**VI. PERFORMANCE ANALYSIS**

The computational cost, the communicational cost and the memory requirement of the proposed scheme is being analysed in this module. The Liao and Hsiao's scheme [26] is also compared here. We imagine that an elliptic curve

with length of 160bits are used in associated schemes, In order to get the same security level. Then the length of an elliptic curve point is 320 bits. The running time of an elliptic curve scale multiplication operation on a 5-MHz tag and a PIV 3 GHZ server is 0.064s and 0.83ms separately [29, 30]. The mandatory running time for the server and the tag when they execute the verification scheme shows the estimation costs. The most complicated operation in both of the proposed scheme and Liao et al.'s scheme is elliptic curve scale multiplication. Here, the estimation cost of those operations could be ignored because we have to compare the number of such operations. Let  $T_{EM}$  represents the running time of an elliptic curve scale multiplication operation. We confirm that the recommended authentication scheme provides a 40 % reduction of the estimation cost compared with Liao and Hsiao's scheme because the computational comparisons between the proposed scheme and Liao et al.'s scheme are listed in Table 1. The cost gives the wide-range of the communicational messages which communicate among the tags and the servers when they execute the verification scheme. The server in the suggested plan sends the message  $m_1 = \{R_1\}$  and  $m_3 = \{R_4\}$  to the tag.

**Table- I: Computational Costs Comparison**

	Liao and Hsiao's scheme	The proposed scheme
The server	5 $T_{EM} \approx 4.15$ ms	3 $T_{EM} \approx 2.49$ ms
The tag	5 $T_{EM} \approx 0.32$ s	3 $T_{EM} \approx 0.192$ s

The cost gives the wide-range of the communicational messages which communicate among the tags and the servers when they execute the verification scheme. The server in the suggested plan sends the message  $m_1 = \{R_1\}$  and  $m_3 = \{R_4\}$  to the tag. Then the server's circulation cost is  $320+320=640$  bits. The tag in the proposed scheme sends the message  $m_2 = \{R_2, C_1\}$  to the server. Then the communicational cost of the tag's is  $320+320=640$  bits. Below here the proposed scheme and Liao et al.'s scheme as listed in Table 2 shows the communicational comparison.

**Table- II: Communicational Cost Comparison**

	Liao and Hsiao's scheme	The proposed scheme
The server	640 bits	640 bits
The tag	640 bits	640 bits
Total	1280bits	1280bits

When the authentication scheme is performed the memory requirement represents the required memory space of the data in the tag side and the server side. To store system parameters  $params = \{q, a, b, P, n\}$ , the tag in the proposed scheme is used.

To store system parameters  $params = \{q, a, b, P, n\}$ , its private key  $y$  and its public key  $R'$ , the server in the illustrated scheme is used. The ID-verifier  $R''$  for each tag is also stored.



Then the storage requirement of the tag is  $160+160+160+320+160+160+320$  w  $= (1,440+320$  w) bits, where w denotes the number of tags in the system. The proposed scheme and Liao's scheme are listed in Table 3 represents the storage requirements comparison.

**Table- III: Storage Cost Comparison**

	Liao and Hsiao's scheme	The proposed scheme
The server	$(1,440+480$ w) bits	$(1,440+320$ w)bits
The tag	1760bits	1600bits
Total	$(3,200+480$ w) bits	$(3,040+320$ w)bits

## VII. CONCLUSION

In our proposed scheme, we have provided with a ECC-based RFID authentication and identification protocol. The proposed protocol can withstand multiple security threats and attacks with much greater efficiency. The results from this analysis can be further used to make sure, the proposed protocol is able to provide robust security and privacy properties and it is able to withstand numerous attacks while it can also overcome various drawbacks seen in previously proposed protocols.

## REFERENCES

- Juels, RFID security and privacy: a research survey, IEEE Journal on Selected Areas in Communication 24 (2006) 381-394.
- C.M. Robert, Radio frequency identification, Computers and Security 25 (2006) 18-26.
- P. Peris-Lopez, A. Orfila, A. Mitrokots, J. van der Lubbe, Journal of Medical Informatics 80 (2011) 13-24.
- S. L. Ting, S. K. Kwok, Albert H. C. Tsang, W. B. Lee, (2011) 657-669.
- Y. Yen, N. Lo, T. Wu, (2012)2769-2778.
- A. Juels, Yoking-proofs for RFID tags, in: First International Workshop on Pervasive Computing and Communication Security, 2004.
- K. Wong, P. Hui, A. Chan, Cryptography and authentication on RFID tags for apparels, Computer in Industry 57 (2005) 342-349.
- Y. Chen, J.-S. Chou, H.-M. Sun, (2008) 2373-2380.
- P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A.Ribagorda, Cryptanalysis verification scheme, (2009) 372-380.
- J. Cho, S. Yeo, S. Kim, securing against brute-force attack (2011) 391-397.
- M. Safkhani, P. Peris-Lopez, J.C. Hernandez-Castro, N. Bagheri, M. Naderi, Cryptanalysis of a hash mutual verification scheme for RFID, Report 2011/311, 2011.
- T. Cao, P. Shen, RFID verification scheme, Journal of Communications 3 (7) (2008) 20-27.
- T.-C. Yeh, C.-H. Wu, Y.-M. Tseng, Computer Communications (34) (2011) 337-341.
- R. Doss, S. Sundaresan, W. Zhou, A practical quadric left over in mobile RFID systems, (2013) 383-396.
- J. Bringer, H. Chabanne, T. Icart, RFID identification protocol. In 7th International Conference -CANS'08, Springer, New York 149-161, 2008.
- T. Deursen, S. Radomirovic, Attacks on RFID protocols (version1.1). Technical Report, August 2009.
- Y. Lee, L. Batina, I. Verbauwhede, Privacy issues in RFID. In The Internet of Things, Giusto D, Lera A, Morabito G,Atzori L (eds): Springer New York, 397-407, 2010.
- C. Lv, H. Li, J. Ma, Y. Zhang, ECC Vulnerability-based RFID authentication protocols, Transactions on Emerging Telecommunications Technologies 23(7) (2012) 618-624.
- R. Peeters, J. Hermans, Attack on Liao and Hsiao's Secure ECC-based RFID verification protocol along with ID-Verifier Transfer Protocol. Cryptology ePrint Archive, Report 2013/399, 2013.

- X. Cao, W. Kou, A Pairing-free Identity-verification scheme along with Minimal Message Exchanges, Information Sciences, 180 (15), 2895-2903, 2010.

## AUTHORS PROFILE



**Sanjeev Kumar** is B.Tech., M.Tech (IT) and pursuing Ph.D. from IIT Dhanbad. He has total 13 years of teaching experience. Now working as, a professor in Department of CSE in ABES Institute of Technology.



**Amulya Bhardwaj** is an undergraduate computer science & engineering student pursuing B.Tech at ABES Institute of Technology, Ghaziabad. His area of interest is Android OS Development and web development. He has done training in Java and Android.



**Gopesh Mittal** is an undergraduate computer science & engineering student pursuing B.Tech at ABES Institute of Technology, Ghaziabad. His area of interest is Web Development and Python. He has done training in Python and JavaScript



**Aditya M. Pillai** is an undergraduate computer science & engineering student pursuing B.Tech. at ABES Institute of Technology, Ghaziabad. His area of interest is Java, android application development. He has done training in Java and Android.