# AN EFFICIENT AND MORE SECURE ID-BASED MUTUAL AUTHENTICATION SCHEME BASED ON ECC FOR MOBILE DEVICES

Shubhangi N. Burde and Hemlata Dakhore

Department of Computer Science and Engineering,
RTMNU University, Nagpur
smathnikar@yahoo.com
hemlata.dakhore@raisoni.net

***ABSTRACT***

*Mobile services are spread throughout the wireless network and are one of the crucial components needed for various applications and services. However, the security of mobile communication has topped the list of concerns for mobile phone users. Confidentiality, Authentication, Integrity and Non-repudiation are required security services for mobile communication. Currently available network security mechanisms are inadequate; hence there is a greater demand to provide a more flexible, reconfigurable, and scalable security mechanism. Traditionally, the security services have been provided by cryptography. Recently, techniques based on elliptic curve cryptography (ECC) have demonstrated the feasibility of providing computer security services efficiently on mobile platforms. Islam and Biswas have proposed a more efficient and secure ID-based system for mobile devices on ECC to enhance security for authentication with key agreement system. They claimed that their system truly is more secure than previous ones and it can resist various attacks. However, it is true because their system is vulnerable to known session-specific temporary information attack, and the other system is denial of service resulting from leaking server's database. Thus, the paper presents an improvement to their system in order to isolate such problems.*

***KEYWORDS***

*Authentication, Dynamic ID, Elliptic curve cryptosystem, Session key.*

## 1. INTRODUCTION

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller. The discrete logarithm problem on elliptic curve groups is believed to be more difficult than the corresponding problem in the underlying finite field. The technology can be used, such as Diffie-Hellman and RSA with most public key encryption methods. Elliptic curve cryptography (ECC) is an approach to public key cryptography (PKC) based on the algebraic structure of elliptic curves over finite fields. According to some researchers, Elliptic curve cryptography (ECC) can have high level of security with a 164-bit key than other systems require a 1,024-bit key because ECC helps to establish equivalent security with lower computing power and battery resource usage. It is widely used for mobile

Natarajan Meghanathan et al. (Eds) : ICCSEA, SPPR, VLSI, WiMoA, SCAI, CNSA, WeST - 2014
pp. 175–186, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.4724

applications. Elliptic Curve Cryptosystem (ECC) based remote authentication system has been use for mobile devices. Mobile phones are most common way of communication and accessing Internet based services. However, the security of mobile communication has topped the list of concerns for mobile phone users. In 2009, Yang [6] proposed a system combining elliptic curve and identity-based cryptosystems to enhance security. They claimed that their system's secure against various attacks, such as replay attack, impersonation attack. But in the same year, Yoon [7] pointed out that Yang's system can't withstand impersonation attack. Furthermore, it doesn't achieve perfect forward secrecy property, which is a very important security in evaluating a strong authentication and key agreement protocol. Then, Yoon proposed another system to fix such problems. In 2010, Chen [5] proposed remote mutual authentication system for mobile devices to improve Yang's system. And they also claimed that their system's more secured to authenticate users and remote servers for mobile devices. However, Islam and Biswas [4] in 2011 have provided a security for mobile devices on elliptic curve cryptosystem. Then, they claimed that their system's truly efficient and usable for mobile users in many internet applications or wireless networks. Nevertheless, in this paper, we prove that the Islam's system can't resist known session-specific temporary information and denial of service resulting from leaking server's database attacks. Afterward, we propose an improvement of their system to overcome such entanglements. Besides, our system possesses low power consumption and computation cost than previous systems. Our main ideas aren't using point addition operation between a random point and user's authentication key and not letting random value is stored into server's database to fix recommended problems of Islam's system [4].

## 2. RELATED WORKS

This paper reviews the basic concepts of elliptic curve cryptosystem.

### 2.1 Elliptic Curve Cryptosystem

An elliptic curve's a cubic equation of the form

$$y2 + a1xy + a2y = x3 + a3x2 + a4x + a5, \quad (1)$$

where a1, a2, a3, a4, a5 are real numbers. Elliptic curves over GF (p) are of the form

$$Ep\ (a, b): y2\ (\text{mod } p) = x3+ax+b \text{ mod } p \quad (2)$$

Where a, b $\epsilon$ Fp and (4a3+27b2) mod p$\neq$ 0. Given an integer s $\in$Fp* and a point P $\in$Ep (a, b), the point multiplication s. P over Ep (a, b) can be defined as

$$s \cdot P = P + P + ... + P\_\_\_\_ \text{ s times} \quad (3)$$

After generating Elliptic curve, any number is entered and checked for prime number. If it is not prime number then lower number which is prime is selected as prime number.

### 2.2 Finding points on the curve:

The following algorithm gives the points on the curve Ep (a, b) [1].

```
Algorithm elliptic points (p, a, b)
{
x=0
While(x<p)
{
```

w=(x3+ax+b) mod p
If (w is a perfect square in Zp)
Output ((x, √w), (x,-√w)) x=x+1
}
}

## 3. REVIEW & CRYPTANALYSIS OF ISLAM & BISWAS'S SCHEME

In this section, the paper "A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices [4]" is review & show that their scheme's vulnerable to known session-specific temporary information attack and denial of service resulting from leaking server's database.

### 3.1 Review of Islam and Biswas's Scheme

This scheme includes four phases: system initialization phase, user registration phase, mutual authentication with key session agreement phase & leaked key revocation phase.

Some important notations in this scheme are listed as follows:

- S: The server.
- U: The user.
- IDU: Identity of U.
- AIDU: U's authentication key.
- qS: The private key of server S.
- rU: A secret number chosen by U.
- rS: A secret number chosen by S.
- H (.): A one way secure hash function.
- Kdf: A one way key derivation function.
- OR: OR operation.
- ||: Message concatenation operation.

#### 3.1.1 System Initialization Phase:

The system initialization phase of Islam includes four steps:

Step 1: S selects a base point P with order n & K-bit prime number from the elliptic curve group Gp.

Step 2: S chooses random number qS (master key of the S) from [1, n - 1] and computes the public key QS = qS.P.

Step 3: S chooses a two one-way secure hash function

$$H1: \{0, 1\} \rightarrow Gp \quad (4)$$

$$H2: Gp \times Gp \rightarrow Z^* p \quad (5)$$

And a one way key derivation functions:

$$Kdf: \{0, 1\}^* Gp \times Gp \rightarrow \{0, 1\} k. \quad (6)$$

Step 4: S publishes (Ep (a, b), P, QS, H1, H2, kdf)

### 3.1.2 User Registration Phase:

The user registration phase is proposed only once when the user wants to take part in the system. Islam's scheme involves three steps:

Step 1: U chooses identity IDU = {0, 1} p and submits it to S with some personal secret information via a secure channel.

Step 2: S checks U's IDU. If IDU already exists in the server database, S asks user U for different ID. Thereafter details of registration will be checked by S and computes the authentication key

$$AIDU = qS.\ H1(IDU \parallel X), \tag{7}$$

where $X \in Z^*$ p is a random number chosen by S. S stores the information (IDU, X, status bit) about U to the secure database. S sets the status bit to 1 if the user's logged in, otherwise sets to zero.

Step 3: S returns AIDU to U via secure channel.

In this phase, Islam's scheme stores random value X into server's database. And if information of database is leak, then attackers can modify these random values of many users. Therefore, these users can not login to S at authentication phase & we'll fix this problem in this scheme.

### 3.1.3 Mutual Authentication with Key Session Agreement Phase:

In this phase, authors assume the message communication in this phase is over an open channel.

Step 1. U keys identity IDU and AIDU into the mobile device & randomly chooses a number rU from [1, n - 1], and computes

$$N=R+AIDU \tag{8}$$

$$M=rU.QS \tag{9}$$

Where R = rU. P. U computes the dynamic identity

$$CIDU = IDU \oplus H2(R \parallel AIDU) \tag{10}$$

and sends the message (CIDU, N, M) to S.

Step 2. On receiving (*CIDU*, *N*, *M*), *S* computes

$$R^*=q^{-1}S \cdot M \tag{11}$$

$$AIDU = N - R^* \tag{12}$$

Then, *S* extracts the user's identity by computing

$$IDU = CIDU \oplus H2\ (R^* \parallel AIDU) \tag{13}$$

And checks the validity of *IDU*. If *IDU* is valid, *S* continues to next step, otherwise rejects U's login request.

Step 3 Furthermore, *S* computes

$$AID^*U = qS.\ H1\ (IDU \| X) \tag{14}$$

(*IDU* and *X* are taken from server's Database) and checks $AID^*U = AIDU$. If it doesn't hold, the server *S* rejects *U*'s login request, otherwise chooses a random number *rS* from [1, n - 1], then computes

$$T = R^* + S \tag{15}$$

$$HS = H2\ (S \| AID^*U) \tag{16}$$

Where $S = rS.\ P$. Now *S* sends the message (*T*, *HS*) to *U*.

Step 4. On receiving (*T*, *HS*), *U* performs $S* = T - R$ and

$$H^*\ S = H2(S \| AIDU) \tag{17}$$

And checks $H^*\ S = HS$. If it holds, *U* authenticates *S* and sends ($H_{RS}$), where $H_{RS} = H2(R \| S^*)$. *U* computes the session key

$$SK = kdf\ (IDU \| AIDU \| K) \tag{18}$$

Where $K = rS.\ R = rS.\ rU.\ P$.

Step 5. On receiving (*HRS*), *S* computes $H^*_{RS}$ =H ($R^* \| S$) and compares it with $H_{RS}$. If it holds, *S* authenticates *U* and computes the session key

$$SK= kdf\ (IDU \| AIDU \| K) \tag{19}$$

Where $K = rS.\ R = rS\ .rU.\ P$. In this phase, the Islam's scheme performs point addition operation between random point R and AIDU. It's very dangerous because if information of any past session's random point R or S is revealed, AIDU will be known by attackers.

### 3.1.4 Leaked Key Revocation Phase:

In this phase, authors assume that AIDU is leaked to an adversary, so user U makes a request to server S for fresh authentication key. U submits the old authentication key AIDU, the identity IDU and personal secret information to S. Now S first checks the validity of U. After validating user's credential, server S selects another random number $X \in Z^*$ p and issues the fresh authentication key AIDU = qS. H1 (IDU ‖ X) with old identity IDU. It's to be noted that the revocation of authentication key doesn't need new identity, only X will be changed in each revocation. S returns the new authentication key AIDU to user U via secure channel. S keeps the database same except that X is replaced by X.

In their leaked key revocation phase, the information of user U is vulnerable to attacks because it's transmitted through open channel. So, the secure channel should be used to protect user U's information when it's submitted in this phase.

## 3.2 Cryptanalysis of Islam and Biswas's Scheme

In this subsection, the paper shows that their scheme's vulnerable to known session-specific temporary information attack & denial of service resulting from leaking server's database.

### 3.2.1 Known Session-Specific Temporary Information Attack:

In paper, the authors mentioned that our scheme can resist known session-specific temporary information attack. In their opinion, when another adversary has the session ephemeral secrets rU and rS, he or she still can't computes session key SK because of lacking of AIDU's information. However, it isn't true because with rU and rS, we'll prove that adversary still can know AIDU's information of user U. For example, adversary A has rU, rS and past package (CIDU, N, M) of another user U, he Or she'll perform following steps to obtain SK.

Step 1: Computes R = rU. P and S = rS. P.
Step 2: Computes AIDU = N - R.
Step 3: Computes IDU = CIDU $\oplus$ H2(R _ AIDU).
Step 4: Computes SK = kdf (IDU || AIDU || K), where K = rU. rS. P.

In Islam's authentication phase, the authors performed point addition operation between a random point R and authentication key AIDU. This is a mistake because if R's information is leaked, user U's AIDU will be easily computed.

### 3.2.2 Denial of Service Resulting From Leaking Server's Database:

In the user registration phase of Islam's scheme, we see that server S store (IDU, X, status-bit) of user U. This is dangerous because if information of server's database is leaked, another adversary can modify X(s)'s value(s). This causes many users not to login to the server S later. Following is the demonstration of this problem.

Step 1: User U sends login message (CIDU, N, and M) to server S.

Step 2: On receiving (*CIDU*, *N*, *and M*) from *U*, *S* computes

$$R^* = q^{-1} S \cdot M \tag{20}$$

$$AIDU = N - R^* \tag{21}$$

$$IDU = CIDU \oplus H (R^* \| AIDU) \tag{22}$$

$$AID^*U = qS \cdot H1 (IDU \| X') \tag{23}$$

Where *X' is* a modified random value of another adversary.

Step 3: S checks if AIDU? = AIDU. Clearly it doesn't hold due to X'. So, S rejects user U. Hence, Islam's scheme's vulnerable to denial of service resulting from leaking server's database. In this scheme, we don't store random value to database to resist this kind of attack.

## 4. PROPOSED AUTHENTICATION SYSTEM

The proposed system will result more efficient enhancements for security on mobile devices using ECC. The proposed system not only inherits the advantages of their system, it also enhances the security. In registration phase, the main goal is achieving AIDU. Random value X helps to resist reregistration of attackers, with the same identity but various authentication keys at different time. In authentication phases, we use two random value rU and rS for server & user to challenge each other. Furthermore, we don't store random value X into database & don't perform point addition operation for AIDU. This system's divided into the four phases of system

initialization, user registration, and mutual authentication with key agreement & leaked key revocation phase.


Figure 1: System Design Model

### 4.1 System Initialization Phase

In this phase, three one-way hash functions are used. The system initialization phase includes four steps:

Step 1: S chooses k-bit prime number p & base point P with order n from the elliptic curve group Gp.

Step 2: S chooses random number qS from [1, n - 1]

Step 3: S chooses three one-way hash functions

$$H1: \{0, 1\}^* \rightarrow Gp \quad (24)$$

$$H2: Gp \times Gp \rightarrow \{0, 1\}^k \quad (25)$$

$$H3: Gp \rightarrow \{0, 1\}^k \quad (26)$$

Step 4: The server publishes (Ep (a, b), P, H1, H2, H3) as system parameters & keeps the master key qS secrete.

### 4.2 User Registration Phase

There are 3 requirements for a registration phase: secrecy for information transmitted between user & server, difference between keys provided for each time of registration by server & server mustn't store user's information which can be a hazardous risk. Easily, Islam's system achieved first two requirements but not the last. So, to recover this point accomplishes a good registration phase. This system consists of 3 steps illustrates these ones.

Step 1: U chooses identity IDU = {0, 1} k and Submits it to S with some personal information via secure channel.

Step 2: S checks U's IDU. If IDU already exists in the server's database, S asks U for different identity. Otherwise, S chooses a random value $X \in Zp^*$. Then, S computes

$$AIDU = qS. H1 (IDU \| X) \quad (27)$$

Finally, S stores (IDU, status-bit) of that user U into database.

Step 3: S returns AIDU to U via a secure channel.

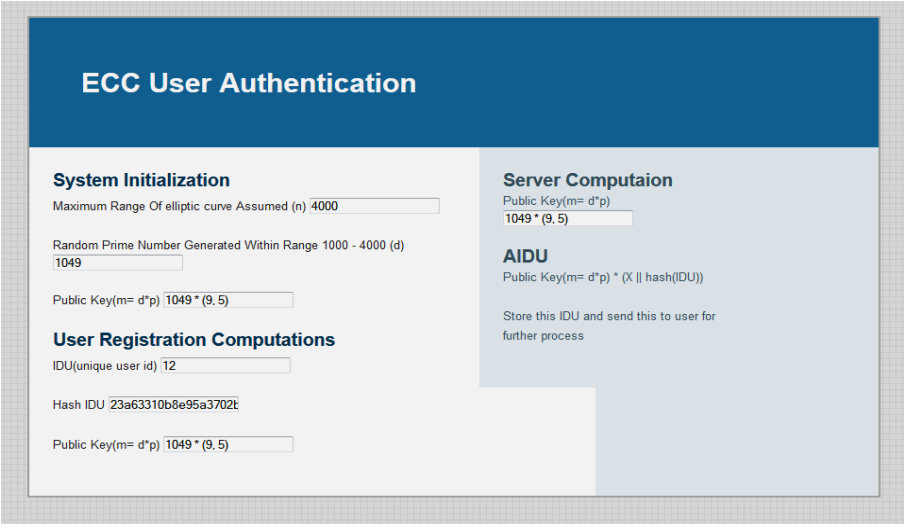


Figure 2: ECC User Authentication

### 4.3 Mutual Authentications & Session Key Agreement Phase

Similarly, this phase also proposes 3 requirements that help authentication be more secure: firstly, user & server must use random values to challenge each other. Secondly, user & server share a secret session key. Finally, temporary information mustn't affect negatively to important information such as authentication key. In Islam's system, both user & server use random values to challenge each other. However, their system's easy to leak authentication key AIDU if any random point's known. Thus, this phase will fix this weak point. In this phase, S and U will have the same session key SK.

Step 1: At first, U keys identity IDU & the authentication key AIDU into the mobile device & randomly choose a number rU from [1, n - 1]. Then, mobile device computes

$$R = rU.\ H1\ (IDU \| X) \tag{28}$$

$$R' = rU.\ AIDU \tag{29}$$

$$M = H2\ (R \| AIDU) \tag{30}$$

$$CIDU = IDU\ OR\ H2\ (R) \tag{31}$$

Mobile device sends (X, CIDU, M, R) to S.

Step 2: On receiving (X, CIDU, M, and R) from U, S computes $R^*$ = qS. R. Then, S extracts user's identity by doing

$$IDU = CIDU\ OR\ H2\ (R^*) \tag{32}$$

and then checks the validity of the identity IDU. If IDU is valid, S continue to go next step, otherwise rejects U's login message request.

Step 3: U computes session key

$$SK = H3\ (X \cdot R^*) \tag{33}$$

Step 5: S authenticates U and computes session key

$$SK = H3 (X \cdot R^*) \quad (34)$$

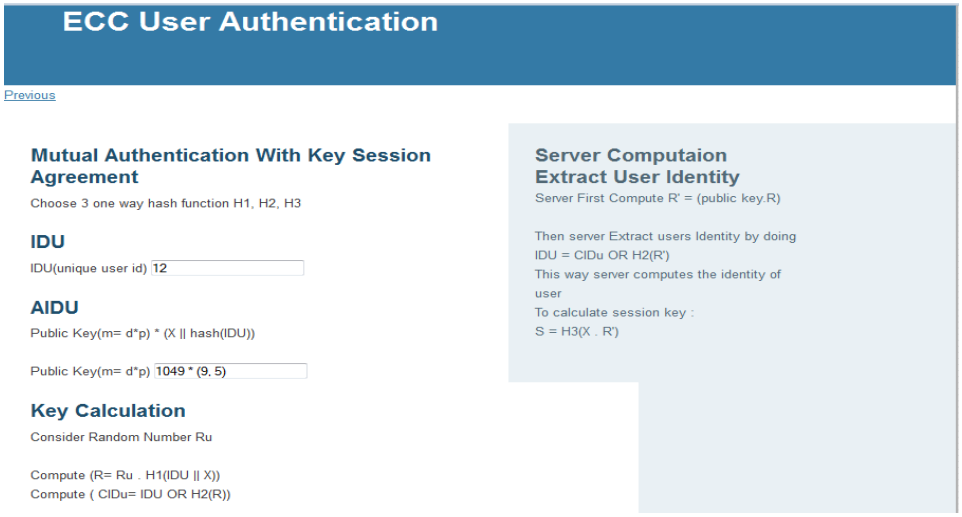


Figure 3: ECC User Mutual Authentication with session Key

### 4.4 Leaked Key Revocation Phase

This phase's similar to Islam's system. However, this phase use a secure channel in two ways to protect secret information of user. And Islam's system doesn't mention secure channel in this phase.

**Research Work in the proposed Scheme:**

The research work is to provide the secure channel integration. Each and every message and its response are passed through secure channel. By secure channel, the request is encoded using encryption method at source end and the request is again decrypted at the destination end by destination's private key. Then the computation of ECC starts. When the response is built, then response creator becomes the source and again encrypts the response. The destination again decrypts the response and then process the response. Base64 encoding schemes are used when there is a need to encode binary data that needs to be stored and transferred over media that are designed to deal with textual data.

The proposed scheme needs less computational amount than previous schemes. The performance of the proposed scheme evaluates in terms computation cost with other schemes. The proposed scheme is more efficient ID-based client authentication scheme for mobile client-server environments.

## 5. SECURITY AND EFFICIENCY ANALYSIS

This section discusses the 2 aspects i.e. security & efficiency of the proposed system.

### 5.1 Security Analysis

Here, various security properties must be considered for the mutual authentication and session key agreement scheme like replay attacks, impersonation attacks, stolen-verifier attacks, mutual

authentication, session key security and perfect forward secrecy, must be considered for the proposed scheme.

### 5.1.1 Replay attack

In the proposed scheme, the freshness of the messages transmitted in the mutual authentication with key agreement phase is provided by the random points RU and RS, and the shared session key k. Only U and S, who can get the session key k and the shared authentication key AIDU can embed the X and the k in the hashed messages generated by U and S respectively. Therefore, the proposed scheme can resist replay attacks.

### 5.1.2 Known Session-Specific Temporary Information Attack

Proposed scheme can resist this kind of attack like Islam's scheme. We assume that another adversary A knows random number of user and server of another past session. However, adversary still can't know session key and user authentication ID. So, adversary can't compute random point to know session key.

### 5.1.3 Stolen-verifier attack

The proposed scheme can withstand stolen-verifier attacks, because S doesn't store any table with information related to U. Server S generates a random value X for each user. Therefore, when authenticating with S, U only needs to send X to S and S uses master key qS to re-construct AIDU of that user. So, S doesn't need to keep U's password in the storage space when a new user's added in the system.

### 5.1.4 Mutual authentication

Mutual authentication means that both the user and server are authenticated to each other within the same protocol. In the proposed scheme, the goal of mutual authentication is to generate an agreed session key k between U and S for particular session. After S receiving the message from U(X, CIDU, M,R) to S. Afterward, S checks $M = H2(R' \| AIDU)$ and U and S authenticate with each other. Therefore, the proposed scheme provides the mutual authentication.

### 5.1.5 Session key security

Session key security means that at the end of the key exchange, the session key is not known by anyone but two communication entities. In proposed scheme, after finishing mutual authentication successfully, both user & server share a session key SK to encrypt message later. So, proposed scheme not only satisfies mutual authentication but also provides session key to partners.

### 5.1.6 Perfect forward secrecy

Perfect forward secrecy means that if a long-term private key (e.g., user password/secret key or server private key) is compromised, this does not compromise any earlier session keys.

### 5.1.7 Lost/Stolen mobile device attack

In proposed scheme, client stores the information into his mobile device, which can help both the client and the server S for mutual authentication. Suppose an adversary steals mobile device, extracts information from the device and then try to get login S by using the extracted information. However, from the adversary cannot extract due to the difficulties of ECDLP problem. Therefore, adversary cannot get any valuable information from the stolen/lost mobile device that can help him to impersonate the client. Thus, the lost/stolen mobile device attack is infeasible to the proposed scheme.

### 5.2 Efficiency Analysis

To analyze computational complexity, compare efficiency between proposed system & the previous systems. That is, let H be the hash function operation, PM be the elliptic curve scalar point multiplication, and PA be the elliptic curve scalar point addition or subtraction. Furthermore, slight difference with Islam's system, the proposed system ignores XOR because it requires very few computations. Clearly, proposed system needs less computational amount than previous systems.

TABLE 1

| Schemes/Computation Type | Yoon[3] | Islam[2] | TRUONG[1] | Proposed Scheme |
|---|---|---|---|---|
| Registration phase | 1PM+1H | 1PM+1H | 1PM+1H | 1PM+1H |
| Mutual authentication phase | 7PM+4PA+ 12H | 7PM+4PA+6H | 7PM + 2PA + 10H | 4PM+2PA+6H |
| Total computation cost | 8PM+4PA+ 13H | 8PM+4PA+7H | 8PM + 2PA + 11H | 5PM+2PA+7H |
| PM: Elliptic curve scalar point multiplication; H: hash operation; PA: Point Addition Operation | | | | |

Figure 3: Efficiency Comparison

## 6. COMPARISION WITH OTHER SCHEME

This section evaluates the performance of the proposed scheme in terms computation cost of proposed scheme with other schemes [2, 3, 4, 5, 6]. To estimate the computation cost of proposed scheme, the following notations are defined: PM is the time complexity to execute elliptic curve scalar point multiplication, H is the time complexity to execute hash operation and PA is the time complexity to execute elliptic curve scalar point addition. It is to be noted that the XOR operation needs very few computations; it is usually neglected considering its computational cost. The computation cost of a scheme is defined by the time spent by the client and the server for registration phase and mutual authentication with session key agreement phase. Besides, proposed scheme avoids the problem of clock synchronization, stolen verifier attack, denial of service attack and achieves users' anonymity as well, which requires two extra OR operations. In addition, the proposed scheme can offer resilience against various attacks such as many logged-in users' attack, lost/stolen mobile device attack, impersonation attack, known session-specific temporary information attack, privileged-insider attack, replay attack, etc. We summarize the computation cost of proposed scheme and carried out a comparison with other schemes in above Table, which shows that proposed scheme is more efficient ID-based client authentication scheme for mobile client-server environments.

## 7. CONCLUSIONS

With the continuous growth of wireless networks, such as GSM, CDPD, 3G and 4G, remote authentication systems play an important role in communicating between parties. After examining the security, implementation and performance of ECC applications on various mobile devices, we can conclude that ECC is the most suitable PKC system for use in a constrained environment. The efficiency and security makes it an attractive alternative to conventional cryptosystems. Consequently, we propose an improved system to eliminate some problems. Also provide the actual implementation of ECC based on the proposed paper. Compared with related systems, the proposed system has the following main advantages: It needs less computational cost. It provides secure user's anonymity. It doesn't hold any verification table. It provides mutual authentication

with session key agreement. As a result, the proposed system's able to provide greater security & be practical in wireless communication system.

## ACKNOWLEDGEMENTS

We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript.

## REFERENCES

[1] Toan-Thinh TRUONG, Minh-Triet TRAN & Anh-Duc DUONG, "Improvement of the more efficient and secure ID-based remote mutual authentication with key agreement system for mobile devices on ECC", IEEE 26th International Conference on Advanced Information Networking and Applications Workshops, 2012.

[2] S. H. Islam and G. P. Biswas, "A more efficient and secure id-based remote mutual authentication with key agreement system for mobile devices on elliptic curve cryptosystem", Journal of Systems and Software, vol. 84, no.11, 2011

[3] Eun-jun yoon, Sung-bae choi and Kee-young yoo, "A secure and efficiency id-based authenticated key agreement system based on elliptic curve cryptosystem for mobile devices", International journal of innovative computing, information and control, April 2012.

[4] J.H. Yang, C.C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem", Computers & Security 28, 2011, 138-143.

[5] H. Debiao, C. Jianhua, H. Jin, "An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security", Information Fusion, 2011,

[6] T. H. Chen, Y.C. Chen and W.K. Shih, "An advanced ecc id-based remote mutual authentication system for mobile devices", Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, pp. 116–120, 2010

[7] J. L. Tsai, T.S. Wu, H.Y. Lin and J.E. Lee, "Efficient convertible multi-authenticated encryption system without message redundancy or one-way hash functions", International Journal of Innovative Computing, Information and Control, 2010.

[8] H. Debiao, C. Jianhua, H. Jin, "An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security", Information Fusion, 2011.

[9] J.H. Yang, C.C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem", Computers & Security 28, 2011, 138-143.

[10] E.J. Yoon and K.Y. Yoo, "Robust id-based remote mutual authentication with key agreement system for mobile devices on ecc", IEEE International Conference on Computational Science and Engineering, vol. 2, pp. 2009, 633–640.

[12] M.L. Das, A. Saxena, V. P. Gulati, "A dynamic ID-based remote user authentication system", IEEE Transactions on Consumer Electronics, 2009, 629-631.

## AUTHOR

**Shubhangi N. Burde**
Department of computer science and engineering,G. H. Raisoni Institute of Engineering and technology for Women Nagpur, India smathnikar@yahoo.com