An Efficient and Secure ID-Based Mutual Authentication with Key Agreement Scheme Based on ECC for Mobile Devices

Shubhangi N. Burde
MTech CSE
Department of computer science and engineering,
G.H.Raisoni Institute of Engineering and technology for Women Nagpur, India

Prof. Hemlata Dakhore
Asst. Professor
Department of computer science and engineering,
G.H.Raisoni Institute of Engineering and Technology for Women Nagpur, India

Prof. S. P. Chhaware
Asst. Professor
Department of Computer Technology,
Priyadarshini College of Engineering, Nagpur, India

Abstract- Mobile devices (e.g., cell phone, PDA and notebook PC) have gained increasingly popularity due to their portability nature. People use these small mobile devices to accomplish the electronic transactions anytime and anywhere. Accordingly, it makes human life more convenient.Users can use to access many applications, for example internet banking, online shopping, mobile pay TV, are accomplished on internet or wireless networks. Therefore, secure communications in such wireless environments are more and more important because they protect transactions between users and servers. Especially, users are people vulnerable to attacks and there are many authentication systems proposed to guarantee them. 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.

Index terms- Authentication, Dynamic ID, elliptic curve cryptosystem, Impersonation, Session key.

I. INTRODUCTION

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller.

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create smaller, faster, and more efficient cryptographic keys. Elliptic curve cryptography (ECC) is an approach to public key cryptography (PKC) based on the algebraic structure of elliptic curves over finite fields. The technology can be used in conjunction with most public key encryption methods, such as Diffie-Hellman and RSA. According to some researchers, Elliptic curve cryptography (ECC) can yield a 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 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. Public key cryptography algorithms provide the way to achieve security requirements viz; confidentiality and authentication.

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 an advanced ECC ID-based 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 proposed a more efficient and secure ID-based remote mutual authentication with key agreement system 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. 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].

II. RELATED WORKS

This paper reviews the basic concepts of elliptic curve cryptosystem & introduces 3 computational problems.

A. Elliptic Curve Cryptosystem

An elliptic curve's a cubic equation of the form y2 + a1xy + a2y = x3 + a3x2 + a4x + a5, where a1, a2, a3, a4, a5 are real numbers. The elliptic curve equation is defined as the form of E*p*(a, b): y2 = x3 + ax + b (mod p) over a prime finite field F*p*, where a, b $\in$ F*p*, p > 3, and 4a3+ 27b2 _= 0 (mod p). Given an integer s $\in$ F*p** and a point P $\in$ E*p*(a, b), the point multiplication s.P over E*p*(a, b) can be defined as s. P = *P* + *P* + ... + *P* _ __ _ *s times* .

B. Computational Problems

Generally, the security of ECC based on the difficulties of the following problems.

1) Given two points P and Q over E*p* (a, b), the elliptic curve discrete logarithm problem (ECDLP) is to find an integer s $\in$ F_p* such that Q = s .P.

2) Given 3 points P, s. P, and t. P over E*p* (a, b) for s, t $\in$ F_p*, the computational Diffie-Hellman problem (CDHP) is to find the point (s. t). P over E*p*(a, b).

3) Given two points P and Q = s . P + t. P over E*p* (a, b) for s, t $\in$ F_p*, the elliptic curve factorization problem (ECFP) is to find two points s. P and t. P over E*p*(a, b).

III. 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.

A. 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.
- $\oplus$: Exclusive-or operation.
- ||: Message concatenation operation.

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 *H*1: {0, 1} $*$ $\rightarrow$ *Gp*, *H*2: *Gp* x *Gp* $\rightarrow$ *Z*$*$ *p* and a one way key derivation function *kdf:* {0, 1} $*$ x *Gp* x *Gp* $\rightarrow$ {0, 1} *k*.
- Step 4: *S* publishes (*Ep(a, b)*, *P*, *QS*, *H*1, *H*2, *kdf*)

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 involve 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* . *H*1(*IDU* _ *X*), 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) 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 $N = R + AIDU$, $M = rU . QS$ Where $R = rU. P. U$ computes the dynamic identity $CIDU = IDU \oplus H2(R \_ AIDU)$ and sends the message ($CIDU$, N, M) to S.

• Step 2. On receiving ($CIDU$, N, M), S computes $R* = q-1\ S \cdot M$ and $AIDU = N - R*$. Then, S extracts the user's identity by computing $IDU = CIDU \oplus H2\ (R* \_ AIDU)$ 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 $AID*U = qS\ H1\ (IDU \_ X)$ (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 $T = R* + S$ and $HS = H2(S \_ AID* U)$, 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 $H* S = H2(S \_ AIDU)$ and checks $H* S? = HS$. If it holds, U authenticates S and sends (HRS), where $HRS = H2(R \_ S*)$. U computes the session key $SK = kdf\ (IDU \_ AIDU \_ K)$, where $K = rS. R = rS. rU . P$.

• Step 5. On receiving (HRS), S computes $H* RS = H\ (R* \_ S)$ and compares it with HRS. If it holds, S authenticates U and computes the session key $SK = kdf\ (IDU \_ AIDU \_ K)$, 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.

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 $\bar{X} \in Z* p$ and issues the fresh authentication key $A\bar{I}DU = qS. H1\ (IDU\ ||X)$ *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 $A\bar{I}DU$ to user U via secure channel. S keeps the database same except that X is replaced by $\bar{X}$.

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.

B. 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.

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.

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, M) to server S.

• Step 2: On receiving ($CIDU$, N, M) from U, S computes $R* = q-1\ S \cdot M, AIDU = N - R*, IDU = CIDU \oplus H2\ (R* \_ AIDU)$ and $AID* U = qS \cdot H1\ (IDU \_ X\_)$, 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.

IV. ECC FOR MOBILE DEVICES AND ITS APPLICATIONS

The elliptic curve public-key systems provide relatively small block size, high speed, and high security. The primary advantage that elliptic curve systems have over systems based on the multiplicative group of a finite field (and also over systems based on the intractability of integer factorization) is the absence of a sub exponential-time algorithm (such as those of "index-calculus" type) that could find discrete logs in these groups. Consequently, we can use an elliptic curve group which is smaller in size while retaining the same level of security. Also in RSA cryptosystem, the security increases sub exponentially

whereas in elliptic curve cryptosystem, the security increases directly exponentially. The consequence is smaller key sizes, bandwidth savings, and faster implementations features which are especially attractive for security applications where computational power and integrated circuit space is limited, such as smart cards, PC (personal computer) cards, and wireless devices.

● In paper [1], author provides the security than previous one. The computation and energy costs of the pairing-based systems are higher than those of ECDLP-based systems. Recently, Yang and Chang pointed out some disadvantages in the previous user authentication systems on ECC. Some of these systems do not provide the mutual authentication or the session key agreement between the user and the server. For some applications, the user and the server need a session key to encrypt the secret information for the subsequent communications after they authenticate with each other. To resolve such problems, YC proposed an ID-based remote mutual authentication with key agreement system on ECC. Based upon ID-based concept, YC system has the following advantages: (1) This system does not require additional computations for certificate; (2) This system is not constructed by bilinear-pairings, which is an expensive operation on EC; (3) This system not only provides mutual authentication but also supports a session key agreement between the user and the server; (4) This system is more efficient and practical than the related works.

V. 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

A. 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 function H1: {0, 1} ∗ → Gp, H2: Gp x Gp → {0, 1} k and H3: Gp → {0, 1} k
• Step 4: The server publishes (Ep (a, b), P, H1, H2, H3) as system parameters & keeps the master key qS secret.

B. 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 ∈ Zp*. Then, S computes AIDU = qS. H1 (IDU _ X). Finally, S stores (IDU, status-bit) of that user U into database.
Step 3: S returns AIDU to U via a secure channel.

Secure Channel:

The research work is to provide the secure channel integration. Each and every message and its response is passed through secure channel. By secure channel, the request is encoded using encryption method.

Using symmetric algorithm 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.

C. Mutual Authentication & 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), R_ = rU. AIDU, M = H2 (R|| AIDU) and CIDU = IDU ⊕ H3 (R). 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 ⊕ H3 (R*) 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: S computes the authentication key AID∗ U = qS · H1 (IDU|| X) and checks M? = H2(R*|| AID* U). If it doesn't hold, S rejects U's login request, otherwise chooses a random number rS from [1, n - 1]. Then, S computes point S = rS · AID* U, T = R* + S and HS = H2(S || AID* U).

Now, S sends (T, HS) to U.

4) Step 4: On receiving (T, HS), U computes S* = T - R_ and checks HS? = H2 (S*|| AIDU). If it holds, U authenticates S and sends the message (HRS) to S, where HRS = H2 (R || S*). U computes session key SK = H3 (rU · S*).

5) Step 5: On receiving (HRS), S checks HRS? = H2 (R* || S). If it holds, S authenticates U. S computes session key SK = H3 (rS. R*).

D. 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.

VI. SECURITY AND EFFICIENCY ANALYSIS

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

A. 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.

1. *Replay attack:* A replay attack is an offensive action in which an adversary impersonates or deceives another legitimate participant through the reuse of information obtained in a protocol.

2. *Impersonation attack* : The impersonation attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.

3. *Stolen-verifier attack:* In most applications, the server stores verifiers of users' passwords or secret keys (e.g., hashed passwords) instead of the clear text of passwords or secret keys. The stolen-verifier attack means that an adversary who steals the password-verifier or secret key-verifier from the server can use it directly to masquerade as a legitimate user in a user authentication execution.

4. *Mutual authentication*: Mutual authentication means that both the user and server are authenticated to each other within the same protocol.

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.

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.

B. 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 ignore exclusive-or (⊕) and concatenation (||) operation because it requires very few computations. Clearly, proposed system needs less computational amount than previous systems.

VII. 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 systems.

VIII. REFERENCE

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

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

[3] "High Performance Scalar Multiplication for ECC", Ravi Kishore Kodali, Harpreet Singh Budwal, 2013 IEEE International Conference on Computer Communication and Informatics (ICCCI -2013), Jan. 04 – 06, 2013, Coimbatore.

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

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

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

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

[8] "Security enhancement for a dynamic id-based remote user authentication system", I.-E. Liao, C.-C. Lee, and M.-S. Hwang, IEEE Transactions on Consumer Electronics, vol. 50, pp. 629–631, 2008.

[9] "Further improvement of an efficient password based remote user authentication system using smart cards", E. J. Yoon, Tian et al, IEEE Transactions on Consumer Electronics, vol. 50, pp. 612-614, May 2004.

[10] "A new remote user authentication system using smart cards", M. S. Hwang and L. H. Li, IEEE Transactions on Consumer Electronics, vol.46, pp. 28-30, Feb 2000.

[11] "A novel remote user authentication system for multi-server environment without using smart cards", K.-H. Yeh and N. W. Lo, International Journal of Innovative Computing and Information Control, vol.6, no.8, pp.3467-3478, 2010.

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

[13] "An authenticated key exchange protocol for mobile stations from two distinct home networks", H.-L. Wang, T.-H. Chen, L.-S. Li, Y.-T. Wu and J. Chen, International Journal of Innovative Computing Information and Control, 2010.

