Elliptic Curve Cryptography(ECC) Based Two Party Authentication Key Agreement Protocol Using Self Certified Public Keys

MS Research Thesis

By:

Raja Zahoor Ahmed Khan
783-FBAS/MSCS/F14

Supervisor:

Dr. Shehzad Ashraf Chaudhry
Assistant Professor DCS&SE, FBAS, IIU

Department of Computer Science & Software Engineering

International Islamic University, Islamabad

August 29, 2017

Public key cryptography

Computer security

A dissertation submitted to the
Department of Computer Science & Software Engineering,
International Islamic University, Islamabad
as a partial fulfillment of the requirements
for the award of the degree of
Master of Science in Computer Science.

INTERNATIONAL ISLAMIC UNIVERSITY ISLAMABAD
FACULTY OF BASIC & APPLIED SCIENCES
DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

Date: ____________

Final Approval

It is certified that we have read this thesis, entitled "**Elliptic Curve Cryptography based two Party Authentication Key Agreement Protocol using self Certified Public Keys (ECC)**" submitted by **Mr. Raja Zahoor Ahmed Khan,** Registration No.**783-FBAS/MSCS/F14**. It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University Islamabad for the award of the degree of Master of Science in Computer Science.

Committee

External Examiner:

Dr. Muazzam A. Khan Khattak, ____________ 7/8
Assistant Professor,
Department of Computer Engineering,
College of E&ME,
National University Science & Technology (NUST), Islamabad

Internal Examiner:

Dr. Syed Husnain Abbas Naqvi, ____________
Chairman,
Department of Computer Science & Software Engineering
FBAS, IIUI

Supervisor:

Dr. Shehzad Ashraf Ch. ____________
Assistant Professor,
Department of Computer Science & Software Engineering,
FBAS, IIUI

Chairman:

Dr. Syed Husnain Abbas Naqvi ____________
Chairman,
Department of Computer Science & Software Engineering
FBAS, IIUI

Declaration

I hereby declare that this thesis, neither as a whole nor as a part thereof has been copied out from any source. It is further declared that no portion of the work presented in this report has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Raja Zahoor Ahmed Khan

Acknowledgments

I am very grateful to *ALLAH* the *ALMIGHTY* for without His grace and blessing this study would not have been possible.

Foremost, I would like to express my sincere gratitude to my supervisor *Dr. Shehzad Ashraf Chaudhry* for the continuous support of my MS study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my MS study.

I would also like to acknowledge my friends, and colleagues. All of them encouraged and provided logistic and technical help during this research.

I would like to admit that I owe all my achievements to my truly, sincere and most loving parents and friends who mean the most to me, and whose prayers have always been a source of determination for me.

Abstract

Improved ECC Based Two-Party Authentication Key Agreement Protocol using Self-certified public Keys of the entities have been proposed in this thesis. Self affirmed open keys are helpful for securing open system. It has crucial role to secure the public channel. In ECC the use of low entropy parameters makes it a suitable candidate to design such authentication protocol. In prior a few ECC based two gathering confirmation conventions with PKI or ID-base have been planned but they have many security lacks and limitations such as heavy computation for managing public key certificate and Isolated key escrow issue. Secret Key is produced by trusted outsider called PKG. PKG is malicious with MIMA the whole protocol is vulnerable. Girault introduced the trusted outsider called System authority(SA). SA creates client open key comparing to secret key which is referred to the customer in a manner of speaking. Public key generated by both user and SA with mutual understanding. In 2015 Islam and Biswas proposed an ECC Based Two-Party Authentication Key Agreement Protocol using Self-certified public Keys (2PAKA).They guarantee that their plan is secure against every known assault. Notwithstanding, In this thesis it has been shown that there arrangement is weak against key compromise and impersonation attack(K-CI). Their computational cost is also high.Therefore we provide improved ECC Based Two-Party Authentication Key agreement Protocol using Self-certified public Keys. We analyze proposed scheme informally and formally with a threat model Scyther and Ban Logic. Proposed scheme has computationally efficient and secured against all known attacks. The Proposed protocol is provided to be an alternative of Islam and Biswas protocol and other PKI-or IBC-2PAKA protocol.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

ECC Based Two-Party Authentication Key Agreement Protocol using Self-certified public Keys between two parties wishes to communicate with contributory session key in public network. Daffie and Hellman Key exchange protocol [1]is the first approach the user use to exchange the massages. It uses very simple operation to generate the secrete session key between the users. In this approach the authentication is not used. Because of the absence of verification of clients this strategy is powerless against man-in-middle attack (MIMA). The authentication of user is to verify the original user that involve in communication. Later on,several Two party authentication key agreement protocol using self certified keys(2PAKA) protocols [2], [3], [4]proposed to avoid the MIMA in the open literature. The above discussed protocol uses the technique public key infrastructure PKI/PKC-CA to avoid the MIMA attack.These techniques uses the modular exponentiation operation,they need more time for execution. It is time consuming model. It is not suitable for resource limited environment like sensor networks,mobile devices,smart card and PDA. In that environment they have very limited computational capabilities and battery life time is likewise restricted. The 2PAKA protocols based on ECC using elliptic curve cryptography [5] rather than PKI or IBC. The ECC- based 2PAKA protocols [6], [7], [8] are more efficient and reliable then previous PKI based protocols,because they use elliptic curve scalar point multiplication(TEM) instead of modular exponentiation. The ECC used elliptic curve discrete logarithm problem (ECDLP). This strategy is further secure and troublesome then discrete logarithm problem(DLP). The ECC based 2PAKA protocol requires less computation and storage because it uses 160bit key instead of 1024bit key of RSA. 160bit key gives an indistinguishable level of security from RSA 1024bit key. The ECC based-2PAKA protocol needs a trusted third party which manages and generates the certificate called "certificate authority(CA)". It validates and produces the public key of users. It is disadvantage of this protocol, because it needs extra handling and additional storage room for storing and maintaining the open keys and testaments.

Recently,several IBC-based two party authentication key agreement protocol using self certified keys based on ECC protocols have been proposed [9], [10], [11], [8], [12] [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23],these protocols endure the secret key escrow issue because the secret key is known by public key generator. If the PKG is malicious with MIMA then the whole scheme is suffered. In 1991, self-Certified public key cryptography(SG-OKC) proposed by Girault[24] is more Well-organized and better then previous protocols like IBC or PKI, because the trusted outsider System Authority(SA)produce the general population key of entity with signing the identity of the entity. The User by uses its secret key that is computed only by user. This technique is useful because user public key can be verified by user and their is no need to issue any extra authentication issue by system authority(SA). So, the private escrow problem was solved as only user known his private key. As compared with CA-PKC or IBC system the SC-PKC are less overhead, storage space,lower communication and no separate certificate required for computation.

1.1 Our contribution

In 2015 Islam and Biswas proposed a two party authentication key agreement protocol using self certified keys. However after a thorough analysis,its shows that their protocol defenseless against key compromise and impersonation attack(KCI) also their computation cost is high. At that point we proposed a moved forward two party authentication key agreement protocol using self certified keys(2PAKA) protocol based on ECC. In this thesis self guaranteed keys are produced by entity and SA (System Authority) with mutual understanding. The use of self certified keys secure the proposed protocol our public channels. The proposed protocol is secure, user friendly and reasonable for mobile are adoc user due to the following properties:

1. **Secure and understandable:** The proposed protocol is secured against every single known assault and it is improved form of the earliest Two-Party Authentication Key Agreement Protocol using Self-certified public Keys like Islam and Biswas scheme. proposed scheme is also very sample and easily understandable by user.
2. **Low Computation cost:** The proposed protocol computation cost is very low compare to other authentication protocol because it used elliptic curve point multiplication and addition instead of other high compotationally tools like modular exponentiation.
3. **Low communication cost:** The proposed scheme have communication cost is very

low with compare to IBC and PKI based protocol. Proposed protocol communication cost is normally equal to the Islam and Biswas scheme but their protocol is vulnerable to security attacks and computation cost is also high.

4. **Formal Security:** The earliest protocol are checked informally and some schemes check with some old tools but proposed scheme formally check with Scyther Security tool and BAN logic tools. Scyther tools provide the visual display of the security and BAN Logic provide the correctness of the protocol.

1.2 Prefaces

This area depicts the essential foundation of Cryptography,ECC and Hash Function.

1.2.1 Cryptography

Cryptography is characterized as to build plans or conventions that can in any case accomplish certain assignments even in the presence of an enemy. A fundamental assignment in cryptography is to empower entities to impart safely over an open network in a mean that ensures their communications' protection and validness.[25]Cryptography is the study of scientific procedures identified with parts of data security, for example, classification, information respectability, substance verification and information root confirmation. Cryptography provides the instrument necessary to contrivance accuracy, accountahility and confidentiality in communication. Cryptographic outlines are portrayed laterally in three autonomous dimensions:

1. The kind of operations used to exchange plain substance to figure content. All encryption numbers depend on upon 2 Universal models: transposition, in which fragments in the plain substance are fixed up. The central basic is that no data be lost. and substitution, in which each part in the plain substance is mapped into another section.

2. The quantity of keys utilized; If initiator and responder utilize a similar key, the framework is alluded to as single-key, mystery key, or ordinary encryption. In event that the initiator and responder utilize diverse keys, framework is alluded hilter kilter, a symmetric, or open key encryption.

3. The path in which the plain suhstance is prepared; a square figure shapes the information one piece of fragments at any given moment, making a yield disturbed for each

information piece. A stream figure shapes the information parts dependably, making yield one portion at any given moment, as it comes.

1.2.2 Objectives of Cryptography

- **Privacy or confidentiality:** Implies keeping data mystery from everything except the individuals who are approved to see it.
- **Data integrity:** Guaranteeing data has not been modified by unapproved or obscure means element confirmation or recognizable proof verification of the character of a substance (e.g., a man, a work station, a charge card, and so on.).
- **Message authentication** Support the wellspring of data; otherwise called information root validation.
- **Signature** a way to credit data to a protest.
- **Authorization conveyance**, to additional element, of authority authorize to do or be somewhat.
- **Validation:** Intends to give appropriateness of approval to utilize or control data or assets.
- **Access control:** Limiting access to assets to advantaged objects.
- **Certification:** Means the authorization of information by a trusted entity.
- **Time stamping:** Implies copy the season of creation or presence of data.
- **Witnessing:** Implies confirming the construction or presence of data by a substance other than the maker.
- **Receipt:** Mean the affirmation that data has been got, affirmation that administrations have been given.
- **Ownership:** Intends to give a question the lawful appropriate to utilize or exchange an asset to others objects.
- **Revocation:** Withdrawal of confirmation or approval.

1.2.3 Symmetric Key Cryptography

It is in like way called as single (secret) key cryptography. It utilizes a solitary key. At this encryption strategy the sender and recipient needs to concur upon a solitary puzzle (distributed) key. Given a message (plain substance) and the key, encryption crops colossal information, which is around an unclear length from the plain substance was. Unscrambling is the switch of encryption, and uses an ill defined key from encryption. Two or three methodology are utilized as a bit of this game plan like MAC operation, MD5, XOR-Operations,Hash function,SHA-1,Transposition, Substitution,, Random Number Generation, Stenography ,HMAC work and few more.

1.2.4 Asymmetric Key Cryptography

It is correspondingly open key cryptography. It utilizes two keys: open key,it is spread uninhibitedly, which is referred to people generally speaking and utilized for encryption and private key, it is besides called bewilder key, which is known just to the client of that key, utilized for unscrambling. General society and the private keys are identified with each other by any consistent means.In unmistakable words, information blended by one open key can be unscrambled just by its taking a gander at secret key[26].

1.2.5 Hash Function

One of the basic primitives in late cryptography is the cryptographic hash work, regularly casually called a restricted hash work. A hash limit is a computationally fit limit mapping parallel strings of self-confident length to twofold strings of some settled length, called hash-values. The essential thought is that a hash-esteem fills in as a compacted illustrative of an information string.[27] We just say that a capacity that takes discretionary measured information as info and believers it to settled size of information $H : \{0,1\}^* \in Z_p$. The output value is called hash value. Hash function can be defined in following properties:

- Suppose, on any given input value X, the H(X) can be easily computed.
- According to preimage resistance property, on a given value H(X) it's infeasible to compute the value of X.

1.2.6 Elliptic Curve

In 1980 Kobiltz [28] and Miller [29] firstly proposed Elliptic curve as a basis for cryptography. Its operation needs very low cost and low memory as well as low communication compare to other cryptosystem. Lion's share of open key cryptosystem like RSA, D-H utilize either whole number or polynomial number-crunching with extensive numbers/polynomials. They need heavy memory for storing and they take more time for computation and communication also they need more processor for processing their keys and messages. Elliptic curve gives same security littler piece estimate. Elliptic curve is alternative of such cryptosystem .It is not a newer but it not analyzed well before.

1.2.6.1 Genuine Elliptic band

- An elliptic band is characterized by a condition in 2 factors x y, with constants
- consider a cubic elliptic bend of frame $y^2 = x^3 + ax + b$ where x, y, a, b are all real numbers additionally characterized zero point O (at infinity)
- consider set of points $E(x, y)$ that satisfy $4x^3 + 27y^2 \neq 0$

Scalar point addition $P + Q = R$ and equation can be computed as $(x_p, y_p) + (x_q, y_q) = (x_r, y_r)$ where $x_r = (\lambda^2 - x_p - x_q)$, $y_r = \lambda(x_p - x_r) - y_p$ and $\lambda = \frac{y_q, y_q}{x_q - x_p}$
Scalar point multiplication is defined as $nP = P + P + ..., +P$ with equation $\lambda = \frac{3x_p^2 + a}{x_q - x_p}$.
It can be used with Diffie-hellman for key exchange also with DSA, ECIES and etc.

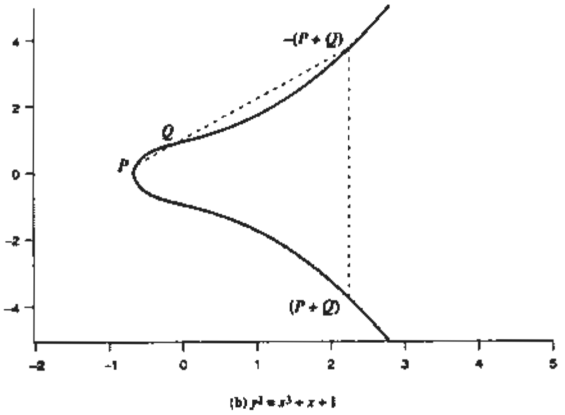


Figure 1.1: Genuine Elliptic Curve Example

1.2.7 Elliptic Curve Cryptography

An open key Cryptography that has small key size but provides equivalent security as compared to non-ECC. ECC security relied on upon the trouble of $ECDLP$. Future, it was extensively recognized in enterprise dissimilar cryptographic scheme for its usefulness in safety, correspondence and calculation and various proficient elliptic curve based PKCs have been proposed. For straightforwardness, some related computationally difficult issues are given underneath:

- **ECC** needs hard problems equiv to discrete logarithmic problem
- **ECDLP**: Given two focuses P and Q. It is computationally hard to compute a scalar K such that
  $Q = kP$
  While Given K and P it is easy to compute
- **ECDHP:** Given three points aP, bP and P. It is computationally difficult to process abP
  While Given a and bP it is anything but difficult to register abP. Similarly given b and aP it is easy to compute abP

1.2.8 Advantages of Elliptic Curve Cryptosystem

- ECC gives more prominent effectiveness around ten times than also whole number factorization frameworks or discrete logarithm frameworks regarding computational overheads, key sizes and data transfer capacity.
- A key size of 4096 bits for RSA offers an indistinguishable level of security from 320 bits in an ECC.

1.3 Outline of Thesis

Further association of proposition is as per the following:

- Chapter 2, provides the literature survey of previous work, detailed review and crypt-analysis of Islam and Biswas scheme, At the end of chapter 2,the problem statement of thesis have been provided.

- Chapter 3, provides the proposed solution and Stages:setup stage,user enrollment stage and key assention stage.
- Chapter 6, provides the security analysis;formal analysis with Scyther security tool and BanLogic and informal analysis against different security requirements have also been provided.
- Chapter 5, provides the performance analysis; analysis have been done on communication, computation cost, running time and comparison with previous work.
- In the last chapter of the research/work has been concluded.

Chapter 2

Literature Review

In 1989, Gunther et al[30] proposed a key trade convention in light of client's character. Each new user first communicate with key authentication center (KAC)then, The entity is able to interchange authenticated keys with other entity on the network.

In 2000 Saeedina, Shahrokh et al[31] proposed the improvement of Gunther identity based key trade convention. They modified their scheme beats the quantity of goes to half, and so limits the correspondence between the parties. This plan gives idealize forward mystery, without extra transmitted information.

In 2002, Hsieh et al [10] planned a Minor alteration in Saeednia identity-based key exchange protocol such that the running time in Saeednia's protocol can be further reduced. However Tseng et al.[12] demonstrated the Hiesh et al scheme cannot restrict the key compromise and impersonation (K-CI) attack. He improved the scheme to limit the K-CI attacks.

Hölbl and Welzer [9] arranged two new two-party ID-based authentication key agreemet conventions.The principal relies on upon Hsieh et al's[10]. scheme what's more, makes it resistant against Tseng et al's[12]. attack, while the second is a capably improved arrangement in light of Tseng's tradition. Zhang et al.[32]proves that Holbl et al.'s[9] protocol cannot repel basic impersonation attack. Their scheme are week against key compromise impersonation (KCI) attacks. They improved their scheme with impersonation attack flexibility and key compromise flexibility.

Smart [33] proposed an ID-based key agreement protocol which utilize Wail pairing its properties and deliberate how they add key conformation. Chen,Kudla [14] and Shim [20] autonomously proposed a legitimate key agreemet(AK)protocols and key agreement with key affirmation(AKC) scheme by altering Smart's AK protocol [33], they also showed that their scheme suggests that it has the perfect forward secrecy assets. Sun and Hsieh [21] showed that Shim and Kudla scheme are weak against key compromise and impersonation (K-CI) attack and man in middle attack (MIMA). They enhanced the Shim and Kudla protocol against these attacks. Ryu et al [19] demonstrate that their scheme minimizes the computation cost and communication cost. It also improves the operational pairing cost to zero. They also proves that their scheme is effective then Kudla's and Chen protocol with similar security properties they have. Choo and Boyd [13] proves that the Ryu et al protocol has not realized on the key compromise impersonation attack (K-CI) reliance properties.

McCullagh and Barreto [18]proves that how their key agreement protocol can be used in either escrowless or escrowed mode. They are described conditions under which clients of various Key Generation midpoints can concur on a common mystery key. Xie [23] validate that McCullagh and Paulo Barreto[18] scheme are weak against key compromise and impersonation attack (K-CI) and they cannot fulfill the criteria of Perfect-Forward- Secrecy properties. They altered this protocol in three way and they say that their schemes are secure against all these attack they mentioned above.

In 2005 Zu-hua at al's [34] proposed bilinear self-certified plan in light of the computational Diffie Hellman suppoysition and Diffie-Hellman issue. Entity can choose secret key self-certified and the public keys and identities of clients can be confirmed indirectly when the public key being produced in a rationally single step. A trusted key generator focus is not required.

Ni, L., Chen, at al,s [35] built up that they can diminish the typical computational bilinear Diffie-Hellman supposition in the irregular oracle demonstrate. They existing two secure variants of the protocol, which are computationally more well-organized then the original scheme. In 2008 Wang,Cao et al[36]put frontward a new ID-based authentication key agreement protocol, which accomplishes PKG forward mystery. They proved that this scheme is more computational efficient than the previously proposed protocol of Chen and Kudla.

In 2005 Tsaur, W. J.[37]proposed elliptic curve cryptography based self-certified public key cryptosystem(ECCSCPKG).They confirmed the validity of public key without signature in certificate base public key cryptosystem. Both session and public keys verified and authenticate in rationally single step. Decrypting cipher,verifying and authenticated public key also finished in logically single step. In 2009 Hölbl and Welzer [38]proposed two new two-party personality based validated key agreement conspire yet their convention was weak against key compromise and impersonation (K-CI) assaults. In 2010 Cao,Kou et al,s planned an identity hased verified key understanding convention which can eliminate bilinear pairings hut their scheme was vulnerable to KSTIA,KOA attack.

In 2012 Wang and Qin [39] arranged enhanced one-to-numerous validation conspire for get to control in pay-TV frameworks but their scheme also proved weak against MS impersonation attack. In 2013 Ni et al[40]proposed effectively secure character based confirmed key agreement conspire in the escrow mode however this convention additionally defenseless against key off set attack(KOA). In 2014 Zhang and Qi[41]proposed an Efficient RFID Authentication Protocol to Enhance Patient Medication Safety Using ECC. Their scheme does not suggest provable security.

2.1 Islam and Biswas scheme review

Islam and Biswas protocol have three stages: Setup stage,User enrollment stage and Key agreement stage.

2.1.1 Setup stage

In setup organize SA makes the structure parameter Ω. It picks a safekeeping constraint $L \in Z^+$ and an elliptic twist accumulate G_q describes the restricted field F_q of prime demand q(m bit distance),where P is the base point,is a big prime number. SA chooses a $s \in Z_q^*$ as a secret key and process the contrasting customer public key $PS = sP$. SA picks the safe three one-way hash functions H_o, H_1, H_2 :$\{0,1\}^* \rightarrow \{0,1\}^L$ at long last circulates the framework paramaters $\Omega = F_q, E/F_q, G_q, P, P_S, H_0, H_1, H_2$

2.1.2 User enrollment stage

At the point when a client I with his character ID_i needs to join the system,he chooses an arbitrary number $x_i \in rZ_q^*$ and then calculates:

$$X_i = (ID_i||x_i)P \tag{2.1}$$

Now the user I send (IDi, Xi) to SA through a dependable channel. The SA selects a $t_i \in rZ_q^*$ for ID_i and computes:

$$P_i = H_0(ID_i||t_i)P_s + X_i \tag{2.2}$$

$$ri = [H_0(ID_i||t_i) + H_0(ID_i||P_i)]s \mod q \tag{2.3}$$

Now SA sends (ID_i, P_i, r_i) to user I through a reliable channel. After receiving (ID_i, p_i, r_i) from SA, client ID_i figures his private key:

$$di = [r_i + H_0(ID_i||x_i)] \mod q \tag{2.4}$$

Then user I verifies the validity of (ID_I, P_i, r_i) by checking that:

$$diP = P_i + H_0(ID_i||P_i)p_s \tag{2.5}$$

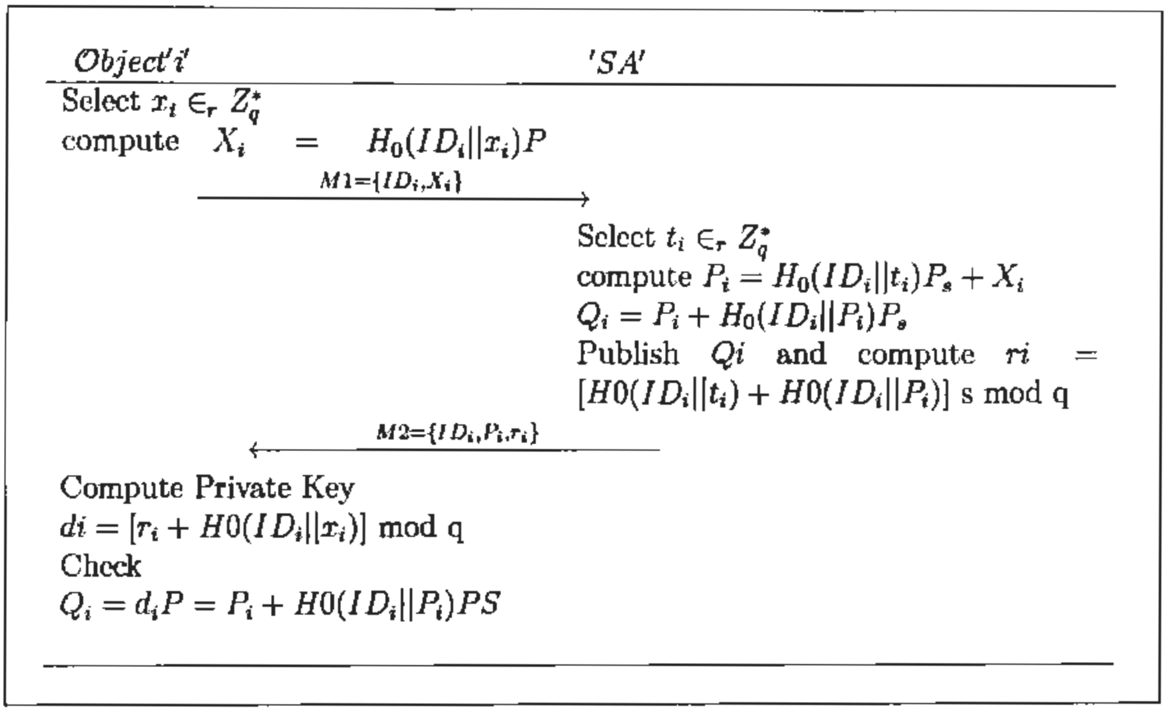
If the equation(2.5)holds then ID_i accepts d_i as his secret key and calculates $Q_i = P_i + H_0(ID_i||P_i)P_s$ as his public key. After enlistment, SA distributes people in general key Q_i of ID_i. It is watched that SA does not have to concern any additional declaration with regard to Q_i. The affirmation of the equation(2.5)is as fallows:

$$\begin{align} d_i &= d_iP \tag{2.6}\\ &= (r_i + H_0(ID_i||x_i)) \tag{2.7}\\ &= [H_0(ID_i||t_i) + H_0(ID_i||P_i)]sP + H_0(ID_i||x_i)P \tag{2.8}\\ &= H_0(ID_i||t_i)_sP + H_0(ID_i||P_i)sP + H_0(ID_i||x_i)P \tag{2.9}\\ &= H_0(ID_i||t_i)P_s + H_0(ID_i||P_i)P_s + X_i \tag{2.10}\\ &= H_0(ID_i||t_i)P_s + X_i + H_0(ID_i||x_i) \tag{2.11}\\ &= P_i + H_0(ID_i||P_i)P_s \tag{2.12}\\ & \tag{2.13} \end{align}$$

Detail of User enrollment stage is illustrated in figure 2.1

2.1.3 Key agreement stage

Recognized that two substances X and Y need to build up a session key among them. It is recognized that the part X goes about as an originator and the substance Y is a respondent.



Object'i' 'SA'

Select $x_i \in_r Z_q^*$

compute $X_i = H_0(ID_i||x_i)P$

$\xrightarrow{M1=\{ID_i,X_i\}}$

Select $t_i \in_r Z_q^*$

compute $P_i = H_0(ID_i||t_i)P_s + X_i$

$Q_i = P_i + H_0(ID_i||P_i)P_s$

Publish Qi and compute ri = $[H0(ID_i||t_i) + H0(ID_i||P_i)]$ s mod q

$\xleftarrow{M2=\{ID_i,P_i,r_i\}}$

Compute Private Key

$di = [r_i + H0(ID_i||x_i)]$ mod q

Check

$Q_i = d_iP = P_i + H0(ID_i||P_i)PS$

Figure 2.1: User enrollment stage of the Islam and Biswas Protocol

By and by the going with two overweight are performed to set up a secret session key among them.

Step-1: Component X play out the followings:
(a)Select $x \in_R Z_q^*$, compute $T_X = xQ_X$ and $R_X = H_1(T_X||d_XQ_Y)$

(b)send (ID_X, T_X, R_X) to Y

Step-2: On receiving $(ID_X, T_X, R_X)$from X,Y resolve:
(a)select $y \in_R Z_q^*$, calculate $T_Y = yQ_Y$ and $R_Y = H_1(T_Y||d_YQ_X)$
(b) Send (ID_Y, T_Y, R_Y) to X

Now entity X computes $R_Y^* = H_1(T_Y||d_XQ_Y)$ contrast and got R_Y, what's more, on the off chance that it is hold, i.e if $R_Y^* = R_Y$,then X computes partial session key as

$$\begin{aligned} K_x &= x d_X T_Y && (2.14)\\ &= x d_X y d_Y P && (2.15)\\ &= x y d_X d_Y P && (2.16) \end{aligned}$$

Similarly, entity Y computes $R_X^* = H_1(T_X||d_Y Q_X)$ and compared with received R_X if $R_X^* = R_X$, then Y calculate the partial session key as

$$\begin{aligned} K_Y &= y d_Y T_X && (2.17)\\ &= y d_Y x d_X P && (2.18)\\ &= x y d_X d_Y P && (2.19) \end{aligned}$$

After fruitful finishing of the above procedure elements X and Y create a typical session key $SK = H_2(ID_x||ID_Y||Trans||K)$ where $k = K_X = K_Y$ and $Trans = (T_X||T_Y||R_X||R_Y)$ feature of the Key agreement stage is exemplified in figure 2.2.

2.2 Cryptanalysis of Islam and Biswas Protocol

The Two-Party authentication key agreement protocol using self certified keys was proposed by Islam and Biswas. It is watched that their tradition is frail against Key compromise and impersonation(K-CI) attack. The cryptanalysis of their Protocol is Followed.

2.2.1 Key Compromise and Impersonation Attack

In Key Compromise Impersonation Attack(K-CI)an adversary X' knows the Private key of element Y. The Adversary X' sends the message to substance Y says I am element x. That sort of assault is known as Key Compromise and Impersonation Attack $(K - CI)$. In this assault the adversary X'tries to mimic the client Y and acquires the session key and found the association between them.

Step-1:The Adversary Perform the following:
Suppose the adversary X' knows the Private key of entity Y. He computes the $T'_X = P$ and computes the $R'_X = H1(T'_X||d_Y Q'_X)$ (b) send (ID'_X, T'_X, R'_X) entity Y

$\mathcal{E}ntity/X'$	$\mathcal{E}ntity/Y'$
Select $x \in_R Z_q^*$ compute $T_X = xQ_X$ $R_X = H_1(T_X \| d_X Q_Y)$	
$\xrightarrow{M1=\{ID_X, T_X, R_X\}}$	
	Select $y \in_R Z_q^*$ compute $T_Y = yQ_Y$ $R_Y = H_1(T_Y \| d_Y Q_X)$
$\xleftarrow{M2=\{ID_Y, T_Y, R_Y\}}$	
$R_Y^* = H_1(T_Y \| d_Y Q_X)$ if $(R_Y^* = R_Y)$ $K_X = (xd_X)T_Y = xyd_Xd_YP$ $SK = H_2(ID_X \| ID_Y \| Trans \| K)$	
	$R_X^* = H_1(T_X \| d_Y Q_X)$ if $(R_X^* = R_X)$ $K_Y = (yd_Y)T_X = xyd_Xd_YP$ $SK = H_2(ID_X \| ID_Y \| Trans \| K)$ Where Trans $=(T_X \| T_Y \| R_X \| R_Y)$ and $K = K_X = K_Y$

Figure 2.2: Key agreement stage of Entity X and Entity Y

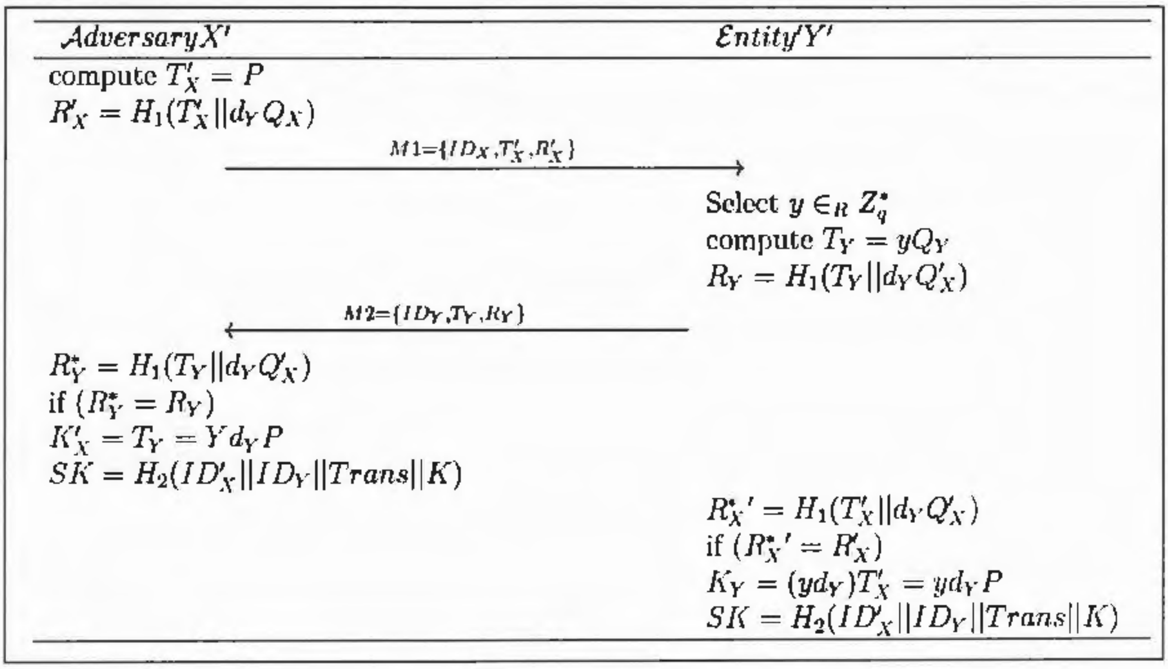

$\mathcal{A}dversaryX'$
$\mathcal{E}ntity/Y'$
compute $T'_X = P$
$R'_X = H_1(T'_X||d_Y Q_X)$
$M1 = \{ID_X, T'_X, R'_X\}$
Select $y \in_R Z_q^*$
compute $T_Y = yQ_Y$
$R_Y = H_1(T_Y||d_Y Q'_X)$
$M2 = \{ID_Y, T_Y, R_Y\}$
$R_Y^* = H_1(T_Y||d_Y Q'_X)$
if $(R_Y^* = R_Y)$
$K'_X = T_Y = Y d_Y P$
$SK = H_2(ID'_X||ID_Y||Trans||K)$
$R_X^*{}' = H_1(T'_X||d_Y Q'_X)$
if $(R_X^*{}' = R'_X)$
$K_Y = (yd_Y)T'_X = yd_Y P$
$SK = H_2(ID'_X||ID_Y||Trans||K)$

Figure 2.3: Key agreement stage of Adversary X' and Entity Y

Step-2:On receiving (ID_X, T'_X, R'_X) from adversary X' entity Y will: (a)The entity Y generates the random number $y \in_R Z_q^*$ and then computes $T_Y = yQ_Y$ And $R_Y = H_1(T_Y||d_Y Q'_X)$ (b) send (ID_Y, T_Y, R_Y) to adversary X'.

After receiving (ID_Y, T_Y, R_Y) the adversary computes the $R_Y^* = H_2(T_Y||d_Y Q'_X)$. If $(R_Y^* = R_Y)$ then adversary computes the partial session key $K = K'_X = T_Y$ then he puts the value of $T_Y, K'_X = yd_Y P$
The adversary X' calculate the Session key $SK = H_3(ID'_X||ID_Y||T'_X||T_Y||R'_X||R_Y||K)$

Similarly after receiving (ID'_X, T'_X, R'_X) the entity Y computes $R_X^*{}' = H_1(T'_X||d_Y Q'_X)$ If $(R_X^*{}' = R'_X)$ then computes the partial session key $K = K_Y = yd_Y T'_X$ put the value of T_x' after that the $K_y = yd_Y P$
The entity Y calculate the session key $SK = H_3(ID'_X||ID_Y||T'_X||T_Y||R'_X||R_Y||K)$ Where $SK = H_3(ID'_X||ID_Y||Trans||K)$ where $K = K'_X = k_Y$ and $Trans = (T'_X||T_Y||R'_X||R_Y)$
Both session keys; Adversary session key and substance Y session key are same. Hence, Islam and Biswas convention are helpless against key compromise and impersonation attack. Detail of Adversary X' and substance Y key agreement Phase have been represented in figure 2.3.

2.3 Problem Statement

Prior 2PAKA conventions in view of ECC and self-confirmed key were proposed. In any case, they were powerless against various sorts of assaults. For that Islam and Biswas proposed the two party authentication key agreement protocol using self certified public keys. They guaranteed that their convention is secure against all assaults. It is watched that their convention is helpless against key compromise and impersonation(K-CI) attack.

2.4 Chapter Summary

This chapter comprehensively provides the literature review, detailed review and cryptanalysis of Islam and Biswas scheme and problem statement of thesis. In this chapter shortly discuss the earlier proposed scheme, their advantages and disadvantages and step by step discussed improved scheme and also their advantages and disadvantages. After that we discussed in detail evaluation of Islam and Biswas protocol. In that protocol we discussed every steps of scheme. In detail cryptanalysis of Islam and Biswas scheme. Here we discussed the limitation and weaknesses of Islam and Biswas scheme and practically we discussed how their scheme is vulnerable to security attacks. and specifically which attack is possible.

Chapter 3

Proposed Scheme

The proposed scheme is an efficient and provably secure,against key compromise impersonation attack (K-CI). This scheme improves the previous two-party authentication key agreement scheme based on ECC and self-certified public keys and removes all security pit fall and security weakness like K-CI.

This proposed scheme has Three stages:

1. Setup stage
2. User enrollment stage
3. Key agreement stage

The setup stage and user enrollment stage are same as the Islam and Biswas scheme. Key agreement stage is different :

3.1 Setup stage

In setup organize SA makes the structure parameter Ω. It picks a safekeeping constraint $L \in Z^+$ and an elliptic twist accumulates G_q describes the restricted field F_q of prime demand q(m bit distance),where P is the base point,is a big prime number. SA chooses a $s \in Z_q^*$ as a secret key and process the contrasting customer public key $PS = sP$. SA picks the safe three one-way hash functions H_o, H_1, H_2 :$\{0,1\}^* \rightarrow \{0,1\}^L$ at long last circulates the framework parameters $\Omega = F_q, E/F_q, G_q, P, P_S, H_0, H_1, H_2$

3.2 User enrollment stage

At the point when a client I with his character ID_i needs to join the system,he chooses an arbitrary number $x_i \in rZ_q^*$ and then calculates:

$$X_i = (ID_i||x_i)P \tag{3.1}$$

Now the user I sends (IDi, Xi) to SA through a dependable channel. The SA selects a $t_i \in rZ_q^*$ for ID_i and computes:

$$P_i = H_0(ID_i||t_i)P_s + X_i \tag{3.2}$$

$$ri = [H_0(ID_i||t_i) + H_0(ID_i||P_i)]s \mod q \tag{3.3}$$

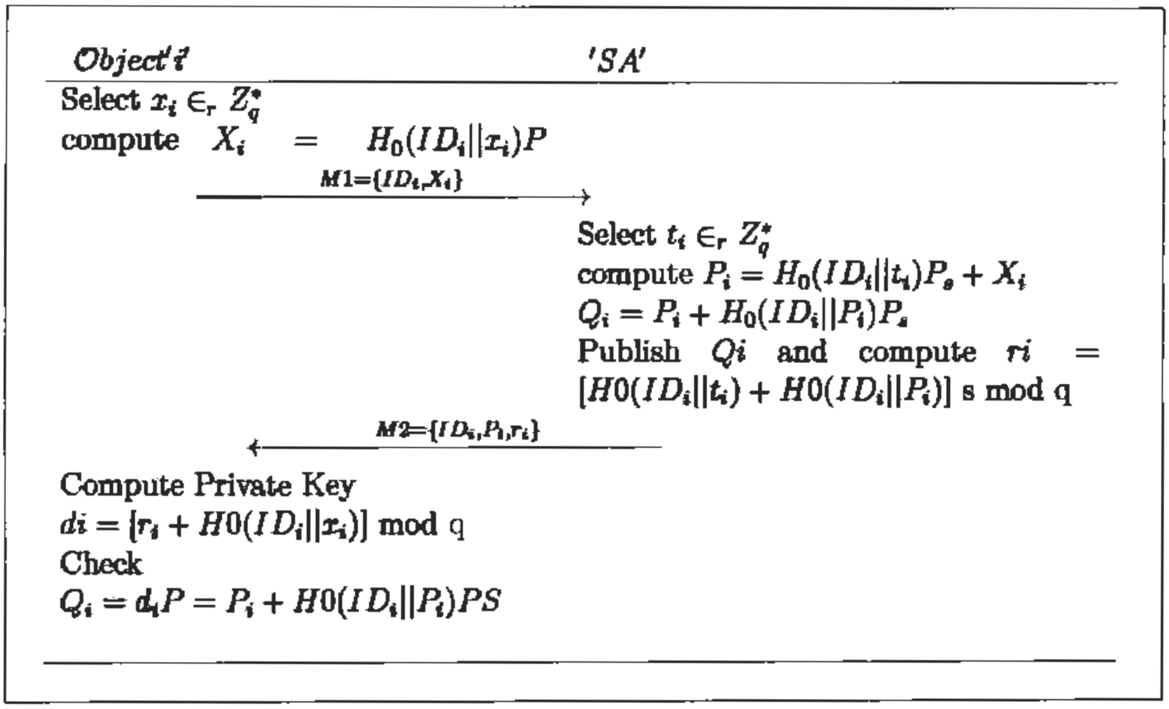
Now SA sends (ID_i, P_i, r_i) to user I through a reliahle channel. After receiving (ID_i, p_i, r_i) from SA, client ID_i figures his private key:

$$di = [r_i + H_0(ID_i||x_i)] \mod q \tag{3.4}$$

Then user I verifies the validity of (ID_I, P_i, r_i) by checking that:

$$diP = P_i + H_0(ID_i||P_i)p_s \tag{3.5}$$

If the equation(2.5)holds then ID_i accepts d_i as his secret key and calculates $Q_i = P_i + H_0(ID_i||P_i)P_s$ as his public key. After enlistment, SA distributes people in general key Q_i of ID_i. It is watched that SA does not have concern to any additional declaration with regard to Q_i. The affirmation of the equation(2.5)is as fallows:



Object'i'
'SA'
Select $x_i \in_r Z_q^*$
compute $X_i = H_0(ID_i||x_i)P$
$M1=\{ID_i,X_i\}$
Select $t_i \in_r Z_q^*$
compute $P_i = H_0(ID_i||t_i)P_s + X_i$
$Q_i = P_i + H_0(ID_i||P_i)P_s$
Publish Qi and compute $ri = [H0(ID_i||t_i) + H0(ID_i||P_i)]$ s mod q
$M2=\{ID_i,P_i,r_i\}$
Compute Private Key
$di = [r_i + H0(ID_i||x_i)]$ mod q
Check
$Q_i = d_iP = P_i + H0(ID_i||P_i)PS$

Figure 3.1: User enrollment stage of proposed scheme

$$
\begin{aligned}
d_i &= d_iP && (3.6)\\
&= (r_i + H_0(ID_i||x_i)) && (3.7)\\
&= [H_0(ID_i||t_i) + H_0(ID_i||P_i)]sP + H_0(ID_i||x_i)P && (3.8)\\
&= H_0(ID_i||t_i)_sP + H_0(ID_i||P_i)sP + H_0(ID_i||x_i)P && (3.9)\\
&= H_0(ID_i||t_i)P_s + H_0(ID_i||P_i)P_s + X_i && (3.10)\\
&= H_0(ID_i||t_i)P_s + X_i + H_0(ID_i||x_i) && (3.11)\\
&= P_i + H_0(ID_i||P_i)P_s && (3.12)\\
& && (3.13)
\end{aligned}
$$

Detail of User enrollment stage is illustrated in figure 3.1

3.3 Key agreement stage

Recognized that two substances X and Y need to build up a mystery session key among them. It is recognized that the part X goes about as an originator and the substance Y is a respondent. By and by the going with two overweight are performed to set up a private session key among them.

Step-1:Entity X selects a random number $x \in_R Z_p^*$ compute $T_X = xP$ and sends (ID_X, T_X) to Y

Step-2: On receiving $(ID_X, T_X)$from X,Y will:
Entity Y selects a random number $y \in_R Z_p^*$, calculate $T_Y = yP$ and Send (ID_Y, T_Y) to X

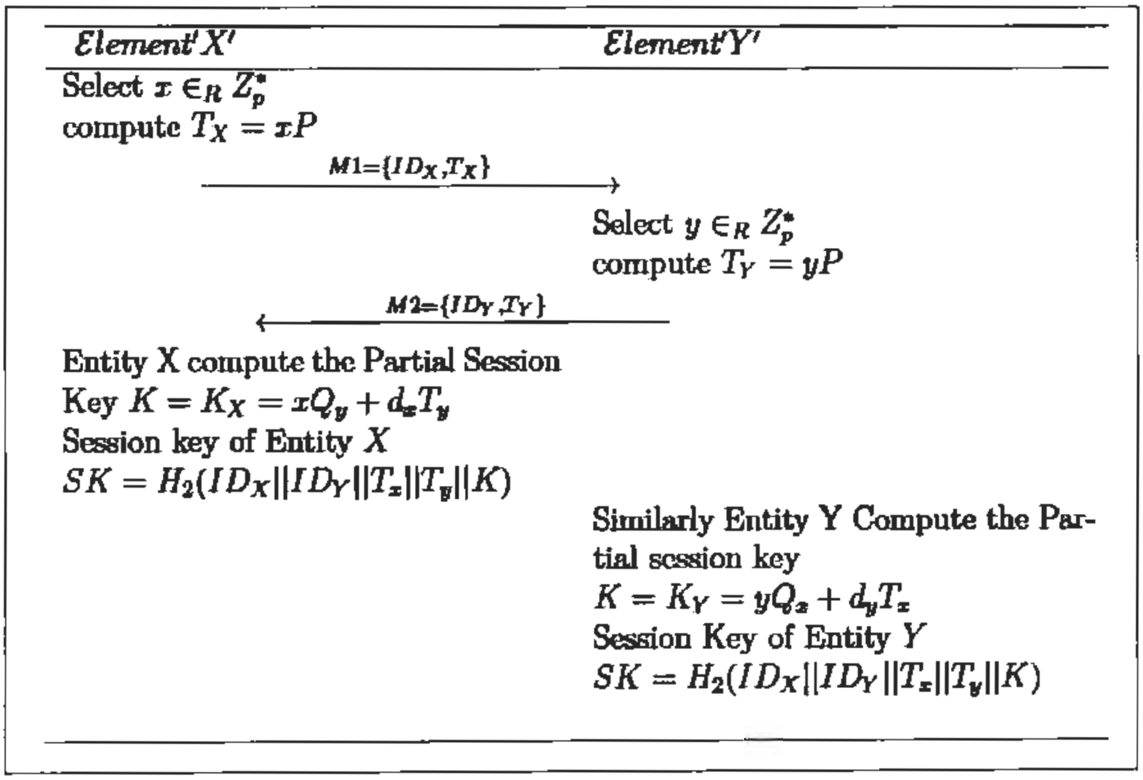
Now entity X calculates the partial session key as

$$K = K_x = xQ_y + d_xT_y \tag{3.14}$$

Similarly, entity Y calculate the partial session key as

$$K = K_Y = yQ_x + d_yT_x \tag{3.15}$$

After fruitful finish of the above procedure elements X produces the session key $SK = H_2(ID_x||ID_Y||T_x||T_Y||K)$ Similarly element Y produce the session key $SK = H_2(ID_x||ID_Y||T_x||T_Y||K)$ Both session key are same. Element X and Element Y are now communicating each other. Detail of Proposed scheme Key assention stage is illustrated in figure (3.2).



Element'X'	*Element'Y'*
Select $x \in_R Z_p^*$ compute $T_X = xP$	
$\xrightarrow{M1=\{ID_X,T_X\}}$	
	Select $y \in_R Z_p^*$ compute $T_Y = yP$
$\xleftarrow{M2=\{ID_Y,T_Y\}}$	
Entity X compute the Partial Session Key $K = K_X = xQ_y + d_xT_y$ Session key of Entity X $SK = H_2(ID_X\|\|ID_Y\|\|T_x\|\|T_y\|\|K)$	
	Similarly Entity Y Compute the Partial session key $K = K_Y = yQ_x + d_yT_x$ Session Key of Entity Y $SK = H_2(ID_X\|\|ID_Y\|\|T_x\|\|T_y\|\|K)$

Figure 3.2: Key agreement phase of Proposed scheme

3.4 Chapter Summary

This chapter provides the proposed scheme of thesis and all steps of proposed scheme in detail. In this section, first we examined the productivity and security of proposed plan and secure against known assaults which are conceivable in prior convention then we talked about the each progression of plan like setup stage, client enrollment stage and key agreement stage in detail.Setup and client enlistment stage are same as Islam and Biswas plot yet key understanding stage is distinctive. In key understanding stage we examine each progression in detail. At that point we without a doubt say that proposed plan is proficient and secure contrast with prior conventions.

Chapter 4

Security Analysis

In this chapter proposed protocol analyzes formally with BAN logic model and Scyther tool. Informally proposed scheme checks against every known attacks, also, think about the security examination of proposed plan with before convention.

4.1 Formal Security examination of the Proposed Protocol with BAN Logic Model

In 1990 Burrows et al[42] proposed the BAN Logic authentication model. This model defines simple but sound and commanding tools based on which the cryptographic protocol can be analyzed more careful then any informal method. In this segment we analyze and explain the accuracy of proposed convention utilizing the BAN Logic display in demonstrated one as follows.

4.1.1 Definition of BAN Logic Model

This section explains the basic syntax,inference and semantics rule used in BAN Logic Model(Barrows et al[42] and Yang and Li[43]. In this section X and Y Signify the principles where Qx and Qy denote the public keys, and dx,dy signify the correspondence secret keys (private key).

4.1.2 Basic notations and descriptions

In this area we Provisionally characterized basic documentations and semantics of the BAN Logic display as takes after.

$(N1)[P\setminus \equiv X]$: P accepts $X]$:or, then again P would be fit the bill for trust X. In particular, P can take X as real.

$(N2)[P \triangleleft X]$: [P sees X] P has become some message X and is prepared for examining and repeating it.

$(N3)[P \setminus \square X]$: P *once said* X. P at some point or another conveyed something particular including the declaration X. It is not known whether this is a replay, however it is realized that P accepted X when he sent it.

$(N4)[P \setminus \square X]$: P *as of late said* X. This suggests P verbalized X in the present continue running of the tradition.

$(N5)[P\setminus \Rightarrow X]$: P controls X The preeminent P is a specialist on X and should be trusted on this matter. (In Kerberos, S controls K'ab)

$(N6)[\#(X)]$:The message X is *fresh*; that is, X has not been sent in a message at whatever point beforc the present continue running of thc tradition. This is normally valid for *nonces.*

$(N7)[P \overset{Pp}{\rightarrow} Q]$: It infers that Pp is general society key of P and the crosspanding secret key dp will never be found by other excepted P or a component trusted by him.

$(N8)[\{X\}_K$ or $[X]_K]$: This addrcsses the condition X encoded under thc kcy K. This is short for [X]˙K *from* P.

$(N9)[P \overset{k}{\leftrightarrow} Q]$: P and Q may utilize the

shared key K to impart. The key Pp is awesome, In that it will be known just by P and Q.

(N10) $[P \overset{X}{\rightleftharpoons} Q]$: The recipe X is a

secret known just to P and to Q, and conceivably to principles

trusted by them. Just P and Q may utilize X to show their characters to each other. A delineation is a riddle mystery key.

(N11) P/Q: It suggests if P is honest to goodness then Q is substantial.

4.1.3 Ban Rules of Inference

In this section we describe a set of Inference rule of BAN Logic model defined in Burrows et al[42] Yung and Lc[43]

(P1) *Message meaning rules* This lead is related with the illumination of messages and help to clarify the wellspring of the messages. In the event that P trusted P_Q be the $Q's$ open key and get a message $[X]$˙dQ scrambled under $Q's$ private key dQ, then P may settled that Q once said the message X

(P2) The *nonce-verification rule:* rule expresses the check that a message is recent, and hence, that the sender still believes in it. If P believes X is fresh and that Q has said X during the current state of the protocol then P believed that Q believed X that is:

$$\frac{P \text{ believes fresh } (X),\ P \text{ believes } Q \text{ said } X}{P \text{ believes } Q \text{ believes } X}$$

That is, if P believes that X could have been uttered only recently and that Q once said X, then P believes that Q believes X. For simplicity, X should be "cleartext".

(P3) The *jurisdiction rule* decide states that if P trusts that Q has locale over explanation X, then P trusts Q on the trueth of X:

$$\frac{P \text{ accepts } Q \text{ controls } X,\ P \text{ accepts } Q \text{ accepts } X}{P \text{ accepts } X}$$

(P4) If a key sees an equation, then he additionally observes its segments, if he knows the essential keys:

$$\frac{P \text{ sees } (X,Y)}{P \text{ sees } X},\quad \frac{P \text{ sees } (X)_Y}{P \text{ sees } X},\quad \frac{P \text{ believes } Q \overset{K}{\leftrightarrow} P(,) P \text{ sees } [X]_K}{P \text{ sees } X},$$

$$\frac{P \text{ believes } \overset{K}{\mapsto} P,\ P \text{ sees } [X]_K}{P \text{ sees } X},\quad \frac{P \text{ believes } \overset{d}{\mapsto} P,\ P \text{ sees } [X]_{d^{-1}}}{P \text{ sees } X}.$$

Take note of that if P sees X and P sees Y it doesn't take after that P sees (X, Y) since that implies that X and Y were articulated in the meantime.

(P5) Belief rules, The essential P can trust an accumulation of explanations if and just if P trusted each of the announcements independently, i.e:

$$\frac{P \text{ trusts } (X) : P \text{ trusts } (Y)}{P \text{ trusts } (X, Y)}$$

(P6) If one a player in the equation is new, then the whole recipe must be new:

$$\frac{P \text{ trusts fresh}(X)}{P \text{ trusts fresh}(X, Y)}.$$

(P7) Session Key rules, In the event that P trusts the session enter (SK) in crisp and P trusts Q trusts X,then P trusts $[P \overset{SK}{\leftrightarrow} Q]$ that is:

$$\frac{P \text{ trusts fresh}(SK), P\text{believes } (Q)\text{believes} X}{[P\text{believes } P \overset{SK}{\leftrightarrow} Q]}$$

where X is the principle part from which SK is drived.

4.1.4 Synthetic rules

In the BAN Logic model the inference rules and basic suggests help to meet the preferred goals of the cryptographic protocols. Butteyan et al(1998) also drives a set of synthetic rule that can be used to construct cryptographic protocol in a systematic way and to prove the reliability of the protocol. In the proposed protocol listed some of such synthetic rules given below. The notation $R \rightarrow S$ means the formula S is deduced from the formula R.

$(S1)[P\text{sees}X \rightarrow P\text{sees}(X, Y)]$

$(S2)[P\text{believes}Q \setminus \Box X \rightarrow P\text{believes}Q \setminus \Box(X, Y)]$

$(S3)[P\text{believes}Q \setminus \Box X \rightarrow Q\text{sees}X]$

$(S4)[P\text{believes}Q \setminus \setminus \Box X \rightarrow Pbelieves(X)]$

4.2 Examination of the proposed protocol

Based on BAN Logic model we formally verified the correctness and reliability of the proposed protocol.i.e at the end of this section both the user confirm that they establish a fresh session key between them.

4.2.1 Initial assumptions

To investigate the proposed protocol, first of all we list the assumptions about the initial state of the protocol.

$(A1)[X \text{ believes } \xrightarrow{Qy} Y]$

$(A2)[Y \text{ believes } \xrightarrow{Qx} X]$

$(A3)[X \text{ believes } \xrightarrow{Qx} X]$

$(A4)[Y \text{ believes } \xrightarrow{Qy} Y]$

$(A5)[X \text{ believes fresh } Tx]$

$(A6)[Y \text{ believes fresh } Ty]$

$(A7)[X \text{ believes } Y \backslash \Rightarrow Qy]$

$(A8)[Y \text{ believes } X \backslash \Rightarrow Qx]$

$(A9)[X \text{ believes } Y \backslash \Rightarrow Ty]$

$(A10)[Y \text{ believes } X \backslash \Rightarrow Tx]$

4.2.2 Idealized Form

According to the BAN Logic model now we transformed the proposed protocol to an idealized form.

$(I1)[X \longrightarrow Y : Tx]$

$(I2)[Y \longrightarrow X : Ty]$

4.2.3 Goals to be achieved

The main anxiety of proposed protocol is to built the trust between the UserX and UserY such that they can share a common and fresh secret key in each session. Accordingly we need to achieve the accompanying objectives so as to verify the security claim of the proposed convention:

$(G1)[Y \text{ believes } [X \xleftrightarrow{SK} \text{Y}]$

$(G2)[Y \text{ believes } [X \text{ believe } X \xleftrightarrow{SK} Y]$

$(G3)[X$ believes $[X \overset{SK}{\longleftrightarrow}$Y]

$(G4)[X$ believes $[Y$ believe $X \overset{SK}{\longleftrightarrow} Y]$

4.2.4 Verification of the scheme

In this section we examine the idea form of the protocol using the BAN Logic model. The aspect steps are given as following: From (I1) We get the following:

$(V1)[X$ believes $(Tx)]$

$(V2)[Y$ sees $(Tx)]$

$(V3)[Y$ sees $\{Tx_{xP}]$ From (I2) We obtain the following:

$(V4)[Y$ believes $(Ty)]$

$(V5)[X$ sees $(Ty)]$

$(V6)[X$ sees $\{Ty\}_{yP}]$ From (V3) and (A2),on applying message meaning rule (P1), we get

$(V7)[Y$ believes $X \setminus \Box(Tx)]$ from the initial assumptions (A5) and through freshness rules (P6),we obtain

$(V8)[X$ believes fresh $(Tx)]$ From (V7) and (V8) we can say

$(V9)[Y$ believes $X \setminus \setminus \Box(Tx)]$ From (V9) and using the synthetic rule (S4) we get

$(V10)[Y$ believes fresh $(Tx)]$ From (V7),V(10) and through nonce verification rule (P2), we get

$(V11)[Y$ believes (X) believes $(Tx)]$ On applying the belief rule (P5), we get from (V11)

$(V12)[Y$ believes (X) believes $(Tx)]$ On applying the jurisdiction rule (P3), from (V12) and the initial assumption (A12),we get

$(V13)Y$ believes (Tx) Now Y computes Ky and finally the session key SK. From Ky and (V8) on applying the freshness rule (P6), we get

$(V14)[Y$ believes fresh $(Ky)]$ Also from (V16), we get

$(V15)[Y$ believes fresh $(SK)]$ From (V11) and (V15) on applying the session key rule (P7),we obtain

$(V16)[Y$ believes $X \overset{SK}{\longleftrightarrow} Y]$

Due to the symmetry of the protocol. X trust that Y is bound to derive the same belief as

$(V17)[Y$ believes X believes $X \xleftrightarrow{SK} Y]$

From (V6) and the initial assumption (A1), on applying the message meaning rule (P1),we obtain:

$(V18)[X$ believes $Y \backslash \backslash \square(Ty)]$ from thc initial assumption (A4), (A8) and through freshness rule (P6), we get

$(V19)[Y$ believes fresh $(Ty)]$ from (V18) and (V19), we have

$(V20)[X$ believes $Y \backslash \backslash \square(Ty)]$

From (V20) and the synthetic rule (S4), we obtain

$(V21)[X$ believes fresh $(Ty)]$ from (V18),(V21) and through the nonce verification rule (P2) ,we get

$(V22)[X$ believes Y believes $(Ty)]$

from (V22) on applying the belief rule (P5) we obtain

$(V23)[X$ believes Y believes $(Ty)]$ From (A11),(V23) and through the jurisdiction rule (P3) we obtain

$(V24)[X$ believes $Ty]$ The UserX computes Kx and the final session key SK from Kx and (V21) and using the freshness rules (P6), we obtain

$(V25)[X$ believes fresh $(Kx)]$ from (V25) we get

$(V26)[X$ believes fresh $(SK)]$ from (V22), (V25) and using the session key rule (P7), we get

$(V27)[X$ believes $X \xleftrightarrow{SK}$Y]

Due to the symmetry of the protocol, X trust that Y is bound to derive the same (V15)belief as:

$(V28)[X$ believes Y believes X$\xleftrightarrow{SK}$Y]

Thus we have reach the preferred goals (G1),(G2),(G3) and (G4) of the proposed protocol consistent to the equation (V16),(V17),(V27) and (V28) as shown above,and it can be determined that UserX and UserY succcssfully generate a fresh,common and protected session key between them using the protocol presented in proposed thesis.

4.3 Formal Security investigation of the Proposed Protocol with an automated tool Scyther

This section of the thesis shows the security analysis of proposed scheme. It has been examined and approved the proposed scheme,automated security protocol check apparatus Scyther adaptation trade off 0.9.2 on portable PC intel center I5 2.4 GHZ with 2GB RAM. All security prerequisites against various assaults have been examined in detail.

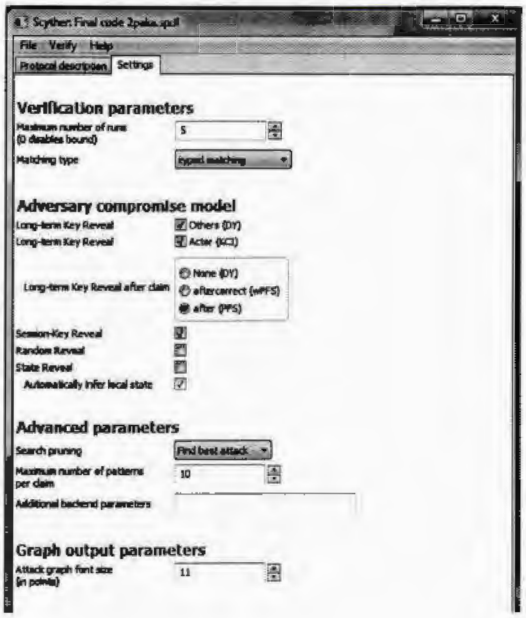
4.3.1 Introduction of Scyther tool

With the development of the Internet and other open systems, countless conventions have been created and composed so as to give safe correspondence. The investigation of such security conventions has ended up being especially troublesome for people, as seen by the way that numerous conventions were observed to be imperfect after sending. Scyther is a push-catch device for the confirmation of the fraud and examination security convention. Scyther gives the cutting edge execution. Device gives graphical UI that suppliment the summon line interface and python script[44].The scyther apparatus display a system for demonstrating enemies security convention examination coming to from a Dolev-Yao effortlessness enemy to all the more effective foes. Enemy models join and rearrange many existing security ideas from both the computational and typical settings. Bolster ideas, for example, powerless flawless forward mystery (PFS), key trade off pantomime (KCI), and enemies fulfilled of state-uncover inquiries[45].

4.3.2 Securtiy Proof with Scyther

Now, the proposed scheme with formal security analysis using automated security verification tool scyther is being discussed. Figure 4.1 shows the setting of adversary model used in verifying the proposed protocol ECC Based 2PAKA protocol. In setting verification parameter, adversary compromise model advance parameter and graphic output parameter setting are shown.

In verification parameter we set maximum number of runs is five and matching type is by default type matching and adversary compromise model we set long term key reveal other (dy) and actor (KCI)both are selected.Select long term reveals after claim is after (PFS) and next we check the session key reveal and automatically infer local state and we unchchecked



Verification parameters

Maximum number of runs (0 disables bound): 5

Matching type: typed matching

Adversary compromise model

Long-term Key Reveal ☑ Others (DY)

Long-term Key Reveal ☑ Actor (KCI)

Long-term Key Reveal after claim: ○ None (DY) ○ aftercorrect (wPFS) ● after (PFS)

Session-Key Reveal ☑

Random Reveal □

State Reveal □

Automatically infer local state ☑

Advanced parameters

Search pruning: Find best attack

Maximum number of patterns per claim: 10

Additional backend parameters:

Graph output parameters

Attack graph font size (in points): 11

Figure 4.1: Scyther Adversary model used for ECC Based 2PAKA protocol verification

the random reveal and state reveal.In advance parameter the selected searching prone is best searched attack and we select the maximum number of claim is ten. In graphic output parameter set the attack font size in point is eleven. These setting are used to analyze proposed protocol.

The researcher models the ECC Based 2PAKA protocol in security protocol description language (SPDL) using Scyther tool. Now let us discuss that what is security protocol description language(SPDL).

Security Protocol Description Language (SPDL):SPDL is an input language for model checker. One vital idea hehind creating SPDL is the ability to check model where several protocol are running. Combining this idea with the semantic concept of using role definations lead to the order. The top lavel consist of the security protocol set monitored by security protocol. The lowest level consist of role definations input to the model checking algorithm is divided into two parts. The first part stated in SPDL supplies the protocol to the model chacker.The second part of the input consists of situation which is used to specify the limit of the model.

SPDL Requirements:SPDL should allow protocol to be specified and security claims to be made about those protocols. It should easy to take a present protocol and create a defination for it. Security protocol description language should be extendable so other expression possiblities could be introduced easily. SPDL should work automatically to someone with some experience in the field of security protocol. Roles communicating with each other should be easily defined by copying reads are sent and modified them. It must be possible to state any protocol which uses asymmetrical or symmetrical encryption and does not require any other term type then agents,nonces,keys,encterms and termlists. SPDL supports two type of comments,single line comment and multiline comments.

Now let us model the ECC Based Two-party authentication key agreement protocol using self certified keys in SPDL using Scyther tools as follows:

```
/*
* ECC based two-party authentication key agreement protocol using self certified PK
*/
// Hash functions
hashfunction H0, H1, H2;

// Addition, multiplication, simply hashes
hashfunction mult,add;

// The protocol description
protocol TWO-PAKA(SA,UserX,UserY)
// UserX = Initiator, UserY = Responder
{
```

```
const P;
role SA // System Authority for Public Key Generation
{
send_1(SA,UserX,P); // Publish public params
send_2(SA,UserY,P);
}


role UserX
 {
  fresh x: Nonce; // Ephemeral/random Secret
  fresh Kx: Nonce; // random Secret

 var Ty: Ticket;
 var Qy; // public key of UserY

 // proposed scheme of Enity X and Entity Y
 recv_1(SA,UserX,P);
 send_3(UserX,UserY, mult(x, P)); // Send Tx = x * P(or IDx)
 recv_4(UserY,UserX,Ty);
 send_5(UserX,UserY,P);
 recv_6(UserY,UserX,Qy);

 // x, Tx = mult(x, P), Ty, P, Qy, dx = sk(UserX)
 claim(UserX,SKR,H2(UserX,UserY,mult(x,P),Ty, add(Kx,mult(x,Qy),mult(sk(UserX), Ty) ) )
}

role UserY
{
 fresh y: Nonce; // Ephemeral/random Secret
 fresh Ky: Nonce; // random Secret

 var Tx: Ticket;
 var Qx; // public key of UserX

 recv_2(SA,UserY,P);
 send_4(UserY,UserX, mult(y, P)); // Send Ty = y * P(or IDy)
 recv_3(UserX,UserY,Tx);
 send_6(UserY,UserX,P);
 recv_5(UserX,UserY,Qx);

 claim(UserY,SKR,H2(UserX,UserY,Tx,mult(y,P), add(Ky,mult(y,Qx),mult(sk(UserY), Tx) ) )
}

}
```

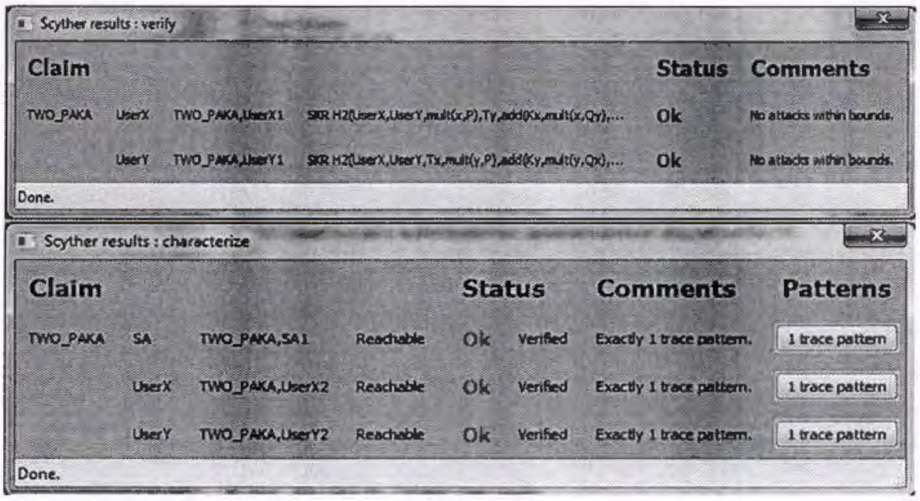
after model the ECC Based Two-party authentication key agreement protocol using self certified keys in security protocol description language using scyther tool the result has been discussed. In output we have verified two thing.

- Verification of claims
- Characterization

Verification of claims: The information dialect of Scyther takes into account portrayal of security properties as far as claim occasions, i.e., in a part necessity one can guarantee that a specific esteem is private (mystery) or certain properties ought to hold for the correspondence pals (validation). Scyther can be utilized to check these properties or distort them.

Characterization: For convention investigation, every convention part can be considered, which implies that Scyther breaks down the convention, and gives a settled portrayal of all fellows that contain an execution of the convention part. By and large, this showing comprises of a modest number (1-5) of conceivable execution designs. By physically analyzing these examples, one can rapidly pick up knowledge in the conceivable issues with the convention and alter it if essential.However the example profundity size is restricted, Scyther can perform unbounded check of the greater part of conventions, as each example speaks to a boundless class of traces.In planning, with conventions from open library, for example, SPORE,Scyther is known to give in around 80 percent of cases either unbounded affirmation or adulteration, and in the other 20 percent gives limited confirmation. The consequence of proposed convention in the wake of testing it from scyther convention appeared in figure 4.2.

Results after verification with Scyther tool



Scyther results : verify

Claim				Status	Comments
TWO_PAKA	UserX	TWO_PAKA,UserX1	SKR H2(UserX,UserY,mult(x,P),Ty,add(Kx,mult(x,Qy)),...	Ok	No attacks within bounds.
	UserY	TWO_PAKA,UserY1	SKR H2(UserX,UserY,Tx,mult(y,P),add(Ky,mult(y,Qx)),...	Ok	No attacks within bounds.

Done.

Scyther results : characterize

Claim				Status		Comments	Patterns
TWO_PAKA	SA	TWO_PAKA,SA1	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	UserX	TWO_PAKA,UserX2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	UserY	TWO_PAKA,UserY2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern

Done.

Figure 4.2: ECC Based 2PAKA Scyther security protocol verification

4.4 Further Security Analysis

Our proposed scheme accomplishes all possible security risks as stated below:

- Key compromise and impersonation(K-CI) attack
- Man-in-the-Middle (MIMA)
- Known-Key Attack(KA)
- Unknown Key-Share Attack(UKA)
- Perfect Forward Secrecy(PFS)
- Known Session-Specific Temporary Information Attack(KSSTIF)
- Key Off set Attack(KOS)
- No Key Control
- Reflection attack(RA)

4.4.1 Key compromise and impersonation(K-CI) attack

In Key Compromise and Impersonation Attack(K-CI)an adversary X' knows the secret key of entity Y. The Adversary X' sends the message to entity Y and says i am entity x. That kind of attack is known as K - CI attack. In this attack the adversary X'tries to impersonate the user Y and obtains the session key and establish the connection between them.

In the proposed protocol,it is assumed that userX secret key dx is Visible to an adversary, and then he tried to imitate userY to userX for locating the resulting session key. The adversary intercept the user X message (IDx, Tx) and then computes $Ty = y.P$ (where y is selected by the adversary)but he cannot compute $Ky = yQx + dyTx$ because with known Tx random number y and the public key Qy , he can compute $KY = YQY + TX$, but he cannot compute $Ky = yQx + dyTx$ because for computing $Ky = yQx + dyTx$ he has to know userY secret key dy. But it is impossible to learn it. So the foe can't have the capacity to compute the session key, thus the proposed protocol is secure against K-CI attack.

4.4.2 Man in the Middle Attack (MIMA)

A sort of security assault in which a malignant foe or aggressor unlawfully embeds himself/herself in two gatherings correspondence and intrudes on their discussion. The enemy can catch the touchy information/data, can send or get information at whatever time and may mimic both sides by envisioning himself/herself a legitimate user.

As affirmed, the proposed convention trades $Tx = x.P$ and $Ty = y.P$ and creates the session key $SK = H2(IDx||IDy||Trans||K)$ utilizing two static mystery keys dx and dy, and two round span keys x and y of the members. Since the customers can affirm Tx and Ty viably, a considerable session key SK is created. Watch that man in center assault is as of late conceivable in our game plan if X' can figure $dxdyP$ from the match $(Qx, Qy) = (dxP, dyP)$ which is irrational as it is hard computational Diffie-Hellman issue. In this way, the planned convention is secure against man in center assault (MIMA).

4.4.3 Known-key attacks

Known-key-ambush is cryptographic attack in which an adversary/attacker can get to the ciphertext. Known-key-ambushes are possibly attempted successfully by a foe/assailant when palintext is associated with ciphertext and enemy could take after plaintext by just performing backtracking.

The ECC based $2PAKA$ tradition fulfills the known key security if information of officially figured session key not empower a foe to exchange off the previous or come up next session keys. Acknowledge that the previous session key delivered by the planned tradition are revealed to an foe X'. In any case, X' can't gather all previous and come up next session keys of the uncovered session key. Decide a previous session key $SK = H2(IDx||IDy||Trans||K)$,$X'$ needs to figure the deficient session key $K = Kx = xQy + dxTy = Ky = yQx + dyTx$ of that session, which depends on upon two transient insider actualities x and y, and the private keys dx and dy of the taking an intrigue components. Tx & Ty of every session are knows to X', and till (dx, dy) and (x, y) are handled from $(Qx\&Qy)$ and $(Tx\&Ty)$, independently, no previous or come up next session keys are exchanged off. Since this figurings incorporate settling $ECDLP$ polynomial time, It is unreasonable as no computation exists in realness. Thus, the known key security stuff is spared in the planned tradition.

4.4.4 Unknown Key Share Attack (U-KS)

Fruitful finishing of a key agreement, an element, userX trusts that a right session key with element userY has been set up in any case, the same may not be consistent with the substance userY and he wrongly trusts that the session key rather than userX has heen built up with a foe X'. Take note of this can't be available in the proposed convention, on the grounds that both client register the basic session key from the confirmation tokens Tx & Ty because of ECDLP, the whole deal secret keys can never be obtained as of general society keys of customers. Subsequently, the planned convention is shielded against obscure keys share assault.

4.4.5 Backward/Forward secrecy

In turn around secret is a sort of puzzle in which a foe X' if aware of new session key he/she would not be capable to get the earlier keys. While the forward puzzle suggests any compromising of old session key should not reveal any future keys for the foe X'.

A key agreement tradition satisfies forward riddle if the security of a once in the past delivered session key is not exchanged off, paying little heed to the likelihood that the private key is no less than one components regardless, not all are known to a foe. Additionally, a tradition has glorify forward secret stuff if an foe knows the secret keys of components can't get any as of now created session key. By and by if the whole deal secret keys dx & dy of userX and userY in the proposed tradition are revealed to an foe X', session enter cannot handled in light of the way that X' needs to surmise the session transient advantaged experiences x and y from Tx and Ty by understanding elliptic band discrete logarithmic issue. Since it is hard to resolvable constrained computation, so our tradition have forward secrecy (PFS).

4.4.6 Known Session-Specific Temporary Information Attack (KSS-TIA)

The safety of made secret key(sk) would not haggled, paying little mind to the likelihood that the session vaporous favored bits of knowledge x and y are spilled to foe X'. In the planned tradition, userX & userY figure sk as $SK = H2(IDx||IDy||Trans||K).X'$ can surmise SK if its knows $K = Kx = xQy + dxTy = Ky = yQx + dyTx$. In any case, X' can't deduce K paying little respect to the likelihood that x and y are revealed, in light of the way that dx and dy are not known to X'. In like manner X' can't get particularly from the match $(Tx, Ty) = (x.P, y.p)$ in light of the fact that it is essential to deal with $(CDHP)$ issue and its not sensitive by a polynomial time restricted estimation. In addition, X' can't use the match (Qx, Qy) to decide the session key SK, in light of the way that it needs to figure $K = Kx = xQy + dxTy = Ky = yQx + dyTx$ from (Qx, Qy), it is troublesome to settle the CDHP. Consequently, it is assumed that the planned tradition guaranteed beside $(KSSTIA)$ attack.

4.4.7 Key Off set Attack

In this attack emulating ambush (KOA/KRA) is a capability of man in middle attack, at this dynamic enemies squares and modify the messages traded among two parts in a session, also maintains the components to concur upon an off course session key, disregarding the way that this strike is not empower to enemy for expand information of the settled session key. Its also encroachment of key uprightness stuff, Its demonstrates any recognized session key would depend upon data sources, swapped using the tradition.Wilson et al[46] raised a two stream checked key agreement tradition lacking key adjustment is displayed to KOA. In proposed tradition the userX and userY exchange (IDx, Tx) and (IDy, Ty) between each otber and a dynamic adversary X' can without a doubt adjust some of these qualities, say Tx and Ty by a dark sort ϵ and produces ϵTx and ϵTy. Things being what they are X'

can't enlist the session keys of userX and userY,they require the data of the whole deal static private keys dx or dy of the substances. Along these lines, the key rehashing strike (KRA) is infeasible in the proposed tradition.

4.4.8 No Key Control

Communicated previously,userX and userY in the planned tradition deliver normal puzzle $SK = H2(IDx||IDy||Trans||K)$. Since $K = Kx = xQy + dxTy = Ky = yQx + dyTx$ and the estimations of x, y in K are picked by the components userX and userY self-assertively, so neither customer nor a foe can realize the session key to be a destined regard or possibly exist in a set having humble number of segments. From now on, it is expressed planned tradition gives (NKC) trademark.

4.4.9 Reflection Attack

The arranged custom has no reflection (RA) and U-KS strike possible, in light of the way that as per Boyed and Choo[47],the elements taking an intrigue substances are joined into the hash work H2, which are utilized to get the standard session key. Furthermore the planned tradition gives brilliance and facts beginning stage approval as the transcription is consolidated into $H2$ work.

4.5 Security Requirements and Comparison

The main purpose of this section is to regulate,analyze and compare the security requirements of the proposed scheme. The subsection elaborates security comparison of proposed scheme with other related work.

4.5.1 Security Requirements

This area gives the correlation of security of the proposed plot with the plans which have been talked about in writing survey and some other examined literature [10],[14],[9],[18],[20],[19][23],[33], [36],[40],[34],[37],[39],[48],[49][50] proposed as of late and the outcome are given in Table . As appeared, none of the plan with the exception of the proposed conspire one can ensure all the security assaults. In any case, the conventions [10],[14],[9] are relatively productive yet they are not secure against KOA/KRA, the reason is that they trade message as xP and xQx without their mark. So the adversary easily launch the KOA/KRA attack on these protocols. The [9] is also insecure against K-CI attack because adversary easily impersonate the legitimate user. The protocol [18] is insecure against PKG-FS,K-CI and KOA/KRA attack. [20] are weak against MIMA and KOA attack. [19] en secure against K-CI and KOA attack. other protocols [23],[33],[36],[40],[51],[37],[39],[48],[49][50] are insecure against MIMA, K-CI, KOA/KRA, KSSTIA attack. Only this proposed protocol is secured against all attack that are mentioned in table 4.1. The detailed comparison is shown in table 4.1.

Protocols	**MIMA**	**PKG-FS**	**K-KS**	**PFS**	**K-CI**	**KSSTIA**	**RA**	**NKC**	**KOA**	**U-KS**	**IA**
Hsieh et al[10]	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y
Chen-Kudla[14]	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
Holbol-Welzer[9]	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y
McCullagh-Barreto[18]	Y	Y	N	N	Y	Y	Y	N	Y	Y	Y
Shim[20]	N	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
Ryu et al[19]	Y	Y	Y	N	Y	N	Y	N	Y	Y	Y
Xie[23]	N	Y	Y	N	Y	Y	Y	N	Y	Y	Y
Smart[33]	Y	Y	N	N	N	Y	Y	N	Y	Y	Y
Cao et al[36]	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y
Cao et al[36]	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y
Zu-hua[34]	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
Ni et al[40]	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
Choie-I[48]	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y
Wang et al[39]	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
Choie-II[48]	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y
Tsaur[37]	Y	Y	N	Y	N	Y	N	N	Y	Y	Y
Choie-III[48]	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y
Kudla-Paterson[49]	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Islam et al[50]	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
proposed protocol	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 4.1: Security Comparison table

Y : Yes provides, N: Does not provide

4.6 Chapter Summary

This part portrays the point by point security investigation of the proposed plot as it has analyzed the scheme formally with BAN logic and an automated tools scyther. Informally with security requirement and in this chapter the security-requirement comparison table has been shown. In formal security analysis first we discussed the security tool BAN logic model its definition and discussed in detail and describe the basic notation of the model then we discussed the BAN logic model rule and inference in detail. after that we analyze the proposed scheme with BAN logic model. And describe the goals that have achieved. Then we verify the protocol. we determine that proposed scheme successfully generate a fresh,common and protected session key between the user. After that we formally check the proposed protocol with an automated security tool scyther. In this section we discuss what is scyther tool and which language they are used then we checked the proposed scheme with scyther code then show the proposed scheme verification result. After that we informally analyze the proposal protocol with known attacks then we discussed the security requirements and comparison of proposed protocol with earlier protocol against different attacks.

Chapter 5

Performance Assessment of Planned Protocol

Execution of some key understanding convention by and large relies on upon the performance of the running with 2 key variables, and a transient presentation of them is given underneath:

- **Computation Cost**

Computation cost,it is the execution cost required to perform different processes and their recurrence involved in producing a common session key between the entities. Since different key agreement methods follow different actions and accordingly the actions like elliptic curve point addition, simple hash operation etc, require relatively smaller computation cost than the operations such as bilinear pairing, elliptic curve scalar point multiplication, modular exponentiation, etc. The computation cost of ECC Based 2PAKA protocols can be reduced if few numbers of expensive tasks are used in their execution. Such protocols have a lead that they are the most appropriate for resource-limited environments such as in smartcards,mobile networks etc.

- **Communication Cost**

The communication cost is another significant factor for measuring the performance of a ECC Based 2PAKA protocol. It comprises the number of rounds, the number of steps per round and message-length used by the entities for creating the authenticated session key between them. The higher is the quantity of communication costs required means to spend more time by contributing entities to establish the session key. The rise in communication cost leads to more communication latency and thus includes more delay in the communicate response phase of the users. For these reasons an ECC Based 2PAKA protocol with high communication cost is inappropriate for telecommunication structure such as online pay-TV,online money transaction, online e-voting, etc., that needs a rapid response for any mandatory service.

- **Communication and computation cost of proposed protocol**

Now we let us calculate the communication and computation cost of the proposed protocol. In proposed protocol the entity X needs to execute two elliptic curve point multiplication and one elliptic curve point addition, Similarly the entity Y also need to execute two elliptic curve point multiplication and one elliptic curve point addition. so The whole protocol need to execute four elliptic curve scalar point multiplication and two elliptic curve point addition.

- **Communication and computation cost comparison with relevant protocol**

Now we analyze some relevant protocol with respect to communication and computation costs. Chen-Kudla protocol[14] perform four pairing operation, four elliptic curve point multiplication two elliptic curve point addition per element. Coa et al protocol[36] required twelve elliptic curve scalar point multiplication. Kudla-Paterson's protocol[49] each element need to perform six modular exponentiation. Expected that all other pairing operation is executed in disconnected mode. Holbl and Welzer protocol -I[9] need to perform eight modular exponentiation and Holbl and Welzer protocol -II[52] required six modular exponentiation to perform. Choie et al protocol-I[48] required six elliptic curve scalar point multiplication(TEM) and four pairing operation(TPAR) for each element. Choie et al scheme-II[48] perform four TEM and eight pairing operation for every element. Smart protocol also required two TEM and two elliptic curve point addition(TEA) every element. Wang et al scheme-I[39] implementing Tate pairing and Wail pairing required four TEM and two pairing based exponentiation operations for every element. Wang et al scheme-II[51] required two pairing operation two TEM and TEA per element to compute common session key. JKar et al[53] protocol required five TEM and one TEA and one simple hash function per element. McCullagh and Barreto scheme[18] perform two TPAR and four TEM and two modular exponentiation per element. Zhu et al protocol[54] required to perform twalve TEM per element. NI et al protocol[40] required one inverse operation four TEM and one TPAR operation per element. Islam et al protocol I[55] required to perform six TEM and four TEA per element.Islam et al protocol II[56]required to perform four TEM and one TEA. Islam et al protocol III[50] also required to perform six TEM and four TEA for every element.

Definition of various operation units	
Notations	Definition and transformation
TEM	Running time of elliptic curve scalar point multiplication,
TEA	Running time of addition of two elliptic curve points,
TEX	Running time of modular exponentiation,
TPAR	Running time of pairing operation,
TIN	Running time of modular inversion operation, TIN
TH	Running time of simple hash function,

Table 5.1: Definition of various operation units

The pairing based two party authentication protocol used either weil pairing or Tate pairing to calculate bi linear pairing operation $e : G1 \times G1 \to G2$ where $G1$ is on added substance amass on elliptic bend E/Fp define over Fp what's more, its request is q,160bits prime and $G2$give proportional level of security of 1024 bits RSA with a 512 bits prime[57] as an estimation cost of matching and one bilinear blending concurring to[58][59] obliged a few time more augmentation then TEM. To approximate the communication cost, it is supposed that the length of the element is 32 bit and production of the hash function is 160 bits. Rendering to Cao et al [36] the longest message which incorporates two focuses in elliptic bend gathering and one personality required $(32 + 2 \times 160)/8 = 44$ bytes transfer speed for correspondence.This research defines a different running time notations and their conversions in mili second[58][59][60][61][18][62]{68[63][50] as shown in table5.3 and demonstrated the quantity of rounds and data transmission required for various related plans have been expected in table 5.3. For conversion in mili second we used the experimental paper of Kilinc et al.[64]We will talk about the execution of the proposed convention as for the cryptographic and math operations utilized for their usage. To ascertain the aggregate computational cost for every convention we accomplished the primitive number-crunching and cryptographic operation timings exhibited in Table 5.2. We used the PBC library (version 0.5.12) [43] which is based on the GMP Library (adaptation 5.0.5). Table 5.2 demonstrates the math mean and the standard deviation of the accompanying primitive operations for thousand executions each;hash function (TH),modular exponentiation (TEX),pairing operation (TPAR),elliptic curve point multiplication (TEM), elliptic curve point addition (TEA),modular inversion operation (TIN).we Saw that a close proportion exists at the OpenSSL library between SHA-1 and modular exponentiation. The timings in Table 5.3 are obtained on a Laptop computer Dell Latitude E5410 which has a Intel Pentium Core I-5 2.4Ghz first generation processor , 2048 MB of RAM and the windows 7 64 bits operating system.

In table 5.3,the communication, computation cost and analysis of different protocol with

PBC Library based Primitive Timing			
Symbols	Operations	Arthimatic Means (ms)	Standard Deviation (ms)
TEM.	Point Multiplication	2.226	0.0000733
TEA.	Point Addition	0.0288	0.0000025
TPAIR.	Pairing	5.811	0.0002854
TEX .	Modular Exponentiation	3.8500	0.0000464
TH	Simple Hash Function	0.0023	0.0000006

Table 5.2: PBC Library based Primitive Timing

Communication and Computation cost				
Protocol	No of rounds	Bandwidth (bytes)	Operations	Runnig time in (ms)
Chen-Kudla[14].	2	$(32 + 512)/8 = 68$	4TPAR + 4TEM + 2TEA	32.2056
Cao et al[36].	2	$(32 + 2 \times 160)/8 = 44$	10TEM + 2TEM	22.712
Choie et al I [48].	2	$(32 + 512)/8 = 68$	4TPAR + 6TEM	36.6
Choie et al II [48].	2	$(32 + 512)/8 = 68$	4TPAR + 8TEM	41.328
Holbl-Walzer I [9].	2	$(32 + 2 \times 1024)/8 = 256$	8TEX	30.8
Holbl-Walzer II [52].	2	$(32 + 2 \times 1024)/8 = 256$	6TEX	23.1
Kudla-Paterson [49].	2	$(32 + 4 \times 1024)/8 = 516$	6TEX	23.1
McCullagh-Barreto [18].	2	$(32 + 512)/8 = 68$	2TPAR + 4TEM + 2TEX	28.226
Wang et al I [39].	2	$(32 + 512)/8 = 68$	2TPAR + 4TEM	20.526
Wang et al II [51].	2	$(32 + 2 \times 512)/8 = 132$	2TPAR + 2TEM + 2TEX	23.774
JKar et al[53].	2	$(32 + 2 \times 160)/8 = 44$	5TEM + 1TEA + TH	11.1611
Zhu et al[54].	3	$(32 + 4 \times 160)/8 = 84$	12TEM	26.722
Islam et al protocol I[55].	2	$(32 + 2 \times 160)/8 = 44$	6TEM + 4TEA + 4TH	13.4564
Islam et al protocol II[56].	2	$(32 + 2 \times 160)/8 = 44$	4TEM + TEA + 2TH	8.9978
Islam et al protocol III[50].	2	$(32 + 2 \times 160)/8 = 44$	6TEM + 4TEA + 4TH	13.4564
Proposed.	2	$(32 + 2 \times 160)/8 = 44$	6TEM + 2TEA + 2TH	13.4182

Table 5.3: Communication and Computation cost

proposed protocol have been shown. The communication cost of the proposed protocol and some other protocols are same. other protocols are vulnerable to security attacks but proposed protocol is secure against all attacks. On the other hand computation cost of the proposed protocol is better then all other protocols have shown in table excepted Islam et al protocol II[56] protocol computation cost is relatively low but their protocol is not secure against some known security attacks.

5.1 Chapter Summary

This chapter describes the detailed performance analysis of the proposed protocol against running time and correspondence cost. Then we calculate the proposed protocol communication and computation cost and comparison this with earlier protocol communication and computation protocol. In table 5.1 we discussed the definition of various operation unit. In table 5.2 describe the PBC library based primitive timing. In table 5.3 we describe the running time and correspondence cost of proposed scheme and analyze it with previous protocol. The running time and correspondence cost of proposed protocol is healthier then the relevant protocol.

Chapter 6

Conclusion

In this thesis, The proposed elliptic curve cryptography(ECC) based two party authentication key agreement protocol using self-certified public keys of the participant has been prepared. Besides the formal security of the proposed plan is approved through a computerized device scyther. The result of this tool shows that no dynamic and uninvolved assault on the proposed plan are conceivable. Another automated tool Ban Logic for correctness of proposed protocol are also used. The results of this tool also verify that the proposed protocol is correct against all active and passive attacks. The security of the proposed protocol has been checked by researcher informally. These analysis also shows that the proposed protocol secure against all known attacks. This protocol is also very efficient in term of communication and running times, which is efficiently operational as a substitute of previous proposed protocol like PKI-identity-based and 2PAKA protocol.

Bibliography

[1] Diffie W, Hellman M. New directions in cryptography. *IEEE transactions on Information Theory* 1976; **22**(6):644–654.

[2] Chen TH, Lee WB, Chen HB. A round-and computation-efficient three-party authenticated key exchange protocol. *Journal of Systems and Software* 2008; **81**(9):1581–1590.

[3] Lu R, Cao Z. Simple three-party key exchange protocol. *Computers & Security* 2007; **26**(1):94–97.

[4] Phan RCW, Yau WC, Goi BM. Cryptanalysis of simple three-party key exchange protocol (s-3pake). *Information sciences* 2008; **178**(13):2849–2856.

[5] Hankerson D, Menezes AJ, Vanstone S. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[6] Pu Q, Zhao X, Ding J. Cryptanalysis of a three-party authenticated key exchange protocol using elliptic curve cryptography. *Research Challenges in Computer Science, 2009. ICRCCS'09. International Conference on*, IEEE, 2009; 7–10.

[7] Tan Z. An enhanced three-party authentication key exchange protocol using elliptic curve cryptography for mobile commerce environments. *Journal of Communications*, Citeseer, 2010.

[8] Tseng YM. An efficient two-party identity-based key exchange protocol. *Informatica* 2007; **18**(1):125–136.

[9] Hölbl M, Welzer T. Two improved two-party identity-based authenticated key agreement protocols. *Computer Standards & Interfaces* 2009; **31**(6):1056–1060.

[10] Hsieh B, Sun H, Hwang T, Lin C. An improvement of saeedniaŠs identity-based key exchange protocol. *Information Security Conference*, vol. 2002, 2002; 41–43.

[11] Saeednia S. Improvement of günther's identity-based key exchange protocol. *Electronics Letters* 2000; **36**(18):1.

[12] Tseng YM. An efficient two-party identity-based key exchange protocol. *Informatica* 2007; **18**(1):125–136.

[13] Boyd C, Choo KKR. Security of two-party identity-based key agreement. *International Conference on Cryptology in Malaysia*, Springer, 2005; 229–243.

[14] Chen L, Kudla C. Identity based authenticated key agreement protocols from pairings. *Computer Security Foundations Workshop, 2003. Proceedings. 16th IEEE*, IEEE, 2003; 219–233.

[15] Chen L, Cheng Z, Smart NP. Identity-based key agreement protocols from pairings. *International Journal of Information Security* 2007; **6**(4):213–241.

[16] Choo KKR, Boyd C, Hitchcock Y, Maitland G. On session identifiers in provably secure protocols. *International Conference on Security in Communication Networks*, Springer, 2004; 351–366.

[17] Li S, Yuan Q, Li J. Towards security two-part authenticated key agreement protocols. *IACR Cryptology ePrint Archive* 2005; **2005**:300.

[18] McCullagh N, Barreto PS. A new two-party identity-based authenticated key agreement. *CryptographersŠ Track at the RSA Conference*, Springer, 2005; 262–274.

[19] Ryu EK, Yoon EJ, Yoo KY. An efficient id-based authenticated key agreement protocol from pairings. *International Conference on Research in Networking*, Springer, 2004; 1458–1463.

[20] Shim K. Efficient id-based authenticated key agreement protocol based on weil pairing. *Electronics Letters* 2003; **39**(8):653–654.

[21] Sun HM, Hsieh BT. Security analysis of shim's authenticated key agreement protocols from pairings. *IACR Cryptology ePrint Archive* 2003; **2003**:113.

[22] Wang S, Cao Z, Choo KKR, Wang L. An improved identity-based key agreement protocol and its security proof. *Information Sciences* 2009; **179**(3):307–318.

[23] Xie G. Cryptanalysis of noel mccullagh and paulo slm barreto¡¯s two-party identity-based key agreement. *IACR Cryptology ePrint Archive* 2004; **2004**:308.

[24] Girault M. Self-certified public keys. *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, 1991; 490–497.

[25] Coron JS. What is cryptography? *IEEE security & privacy* 2006; **4**(1):70–73.

[26] Yang G, Wong DS, Wang H, Deng X. Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences* 2008; **74**(7):1160–1172.

[27] Menezes AJ, Van Oorschot PC, Vanstone SA. *Handbook of applied cryptography.* CRC press, 1996.

[28] Koblitz N. Elliptic curve cryptosystems. *Mathematics of computation* 1987; **48**(177):203–209.

[29] Miller VS. Use of elliptic curves in cryptography. *Conference on the Theory and Application of Cryptographic Techniques*, Springer, 1985; 417–426.

[30] Günther CG. An identity-based key-exchange protocol. *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, 1989; 29–37.

[31] Saeednia S. Improvement of günther's identity-based key exchange protocol. *Electronics Letters* 2000; **36**(18):1.

[32] Zhang S, Cheng Q, Wang X. Impersonation attack on two identity-based authenticated key exchange protocols. *2010 WASE International Conference on Information Engineering*, 2010.

[33] Smart N. Identity-based authenticated key agreement protocol based on weil pairing. *Electronics letters* 2002; **38**(13):630–632.

[34] Zu-Hua S. Efficient authenticated key agreement protocol using self-certified public keys from pairings. *Wuhan University Journal of Natural Sciences* 2005; **10**(1):267–270.

[35] Ni L, Chen G, Li J, Hao Y. Strongly secure identity-based authenticated key agreement protocols. *Computers & Electrical Engineering* 2011; **37**(2):205–217.

[36] Wang S, Cao Z, Cao F, *et al.*. Efficient identity-based authenticated key agreement protocol with pkg forward secrecy. *IJ Network Security* 2008; **7**(2):181–186.

[37] Tsaur WJ. Several security schemes constructed using ecc-based self-certified public key cryptosystems. *Applied Mathematics and Computation* 2005; **168**(1):447–464.

[38] Hölbl M, Welzer T, Brumen B. An improved two-party identity-based authenticated key agreement protocol using pairings. *Journal of Computer and System Sciences* 2012; **78**(1):142–150.

[39] Wang H, Qin B. Improved one-to-many authentication scheme for access control in pay-tv systems. *IET information Security* 2012; **6**(4):281–290.

[40] Ni L, Chen G, Li J, Hao Y. Strongly secure identity-based authenticated key agreement protocols in the escrow mode. *Science China Information Sciences* 2013; **56**(8):1–14.

[41] Zhang Z, Qi Q. An efficient rfid authentication protocol to enhance patient medication safety using elliptic curve cryptography. *Journal of medical systems* 2014; **38**(5):1–7.

[42] Burrows M, Abadi M, Needham RM. A logic of authentication. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 426, The Royal Society, 1989; 233–271.

[43] Yang S, Li X. A limitation of ban logic analysis on a man-in-the-middle attack. *Journal of Information and Computing Science* 2006; **1**(3):131–138.

[44] Cremers CJ. The scyther tool: Verification, falsification, and analysis of security protocols. *International Conference on Computer Aided Verification*, Springer, 2008; 414–418.

[45] Basin D, Cremers C. Modeling and analyzing security in the presence of compromising adversaries. *European Symposium on Research in Computer Security*, Springer, 2010; 340–356.

[46] Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis. *IMA International Conference on Cryptography and Coding*, Springer, 1997; 30–45.

[47] Boyd C, Choo KKR. Security of two-party identity-based key agreement. *International Conference on Cryptology in Malaysia*, Springer, 2005; 229–243.

[48] Choie YJ, Jeong E, Lee E. Efficient identity-based authenticated key agreement protocol from pairings. *Applied Mathematics and Computation* 2005; **162**(1):179–188.

[49] Kudla C, Paterson KG. Modular security proofs for key agreement protocols. *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2005; 549–565.

[50] Islam SH, Biswas G. Design of two-party authenticated key agreement protocol based on ecc and self-certified public keys. *Wireless Personal Communications* 2015; **82**(4):2727–2750.

[51] Wang S, Cao Z, Cheng Z, Choo KKR. Perfect forward secure identity-based authenticated

key agreement protocol in the escrow mode. *Science in China series F: Information sciences* 2009; **52**(8):1358–1370.

[52] Hölbl M, Welzer T. Two improved two-party identity-based authenticated key agreement protocols. *Computer Standards & Interfaces* 2009; **31**(6):1056–1060.

[53] Kar J, Majhi B. An efficient two-party identity-based key exchange protocol based on ecdlp. *IACR Cryptology ePrint Archive* 2009; **2009**:441.

[54] Zhu RW, Yang G, Wong DS. An efficient identity-based key exchange protocol with kgs forward secrecy for low-power devices. *Theoretical Computer Science* 2007; **378**(2):198–207.

[55] Islam SH, Biswas G. An improved pairing-free identity-based authenticated key agreement protocol based on ecc. *Procedia Engineering* 2012; **30**:499–507.

[56] Islam SH, Biswas G. A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks. *annals of telecommunications-annales des télécommunications* 2012; **67**(11-12):547–558.

[57] Ren K, Lou W, Zeng K, Moran PJ. On broadcast authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications* 2007; **6**(11):4136–4144.

[58] Barreto PS, Lynn B, Scott M. On the selection of pairing-friendly groups. *International Workshop on Selected Areas in Cryptography*, Springer, 2003; 17–25.

[59] Barreto PS, Kim HY, Lynn B, Scott M. Efficient algorithms for pairing-based cryptosystems. *Annual International Cryptology Conference*, Springer, 2002; 354–369.

[60] Cao X, Kou W, Du X. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. *Information Sciences* 2010; **180**(15):2895–2903.

[61] Chung YF, Huang KH, Lai F, Chen TS. Id-based digital signature scheme on the elliptic curve cryptosystem. *Computer Standards & Interfaces* 2007; **29**(6):601–604.

[62] Islam SH, Biswas G. A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings. *Journal of King Saud University-Computer and Information Sciences* 2014; **26**(1):55–67.

[63] Xuefei C, Weidong K, Yong Y, Rong S. Identity-based authenticated key agreement protocols without bilinear pairings. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 2008; **91**(12):3833–3836.

[64] Fan AW, Lu SX. An improved elliptic curve digital signature algorithm. *Applied Mechanics and Materials*, vol. 34, Trans Tech Publ, 2010; 1024–1027.