A Review on Distributed System Security using Elliptic Curve Cryptography

Garima Verma, Amandeep Kaur

Department of Computer Science, BBD University, Lucknow

Abstract- Most of the security architecture uses public key cryptosystems for authentication and to secure the communication that takes place on distributes sites. Now a day's identity based cryptography and certificate-less public key cryptography are used for enhancing the security. Certificate-less based cryptography has reduced the certificate necessity for key distribution and reducing the problem of key escrow that arise in identity based cryptography. A review based on identity based and certificate-less based is carried out to show that how they are beneficial in future for enhancing distributed system security using Elliptic curve cryptography.

Index Terms- Certificate-less based cryptography, Elliptic curve cryptography; Identity based cryptography, Public key cryptosystems.

I. INTRODUCTION

Distributed system works as a single system for users even if it is a collection of multiple systems where multiple types or varieties of hardware and software communicate to achieve a goal to perform multiple tasks using some communication over network. This communication involves message passing, sharing resources in a transparent and scalable way.

As communication takes place among geographically distributed sites, therefore authentication is necessary. Resources are also shared and therefore authorization and access policies are required. For secure communication of messages we need some cryptographic algorithms and as now Elliptic curve cryptography is a recent technique for this which is mostly used in two forms as identity based and certificateless based for key agreement.

This paper is divided into four sections. Elliptic curve cryptography in Section II. Section III presents a survey of related work with respect to distributed system. Section IV is the conclusion.

II. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography has been derived from elliptic curve which are in non singular form used for cryptography and has some basic properties. A group is said to be abelian when it includes operation, denoted by •, which is associated with each ordered pair (x, y) of elements in G an element (x • y) in G, as shown in Table below:-

Property	Description
Closure	If x and y belong to G, then x • y is also in G.
Associative	x • (y • z) = (x • y) • z for all x, y, z in G.
Identity element	x • e = e • x = x for all e in G .
Inverse element	There exist an element x' in G such that x • x' = x' • x = e.
Commutative	x·y= y·x for all x, y in G.

Table I. Properties of Abelian group

Number of public key ciphers are based on the use of an abelian group.An abelian group used with an operation of · using two elements that denote x·y which satisfies the group property and the commutative property too.

Miller [53] and Koblitz[52] proposed Elliptic curves in cryptography in 1985 and their research proved that it can be used for security services such as authentication, confidentiality, key exchange, data integrity and more. By 1987, elliptic curves were being implemented in cryptosystems. An improvement over the discrete log method does not directly use the finite fields or groups but rather the elliptic curves defined over them. Elliptic curves allow the encryption of message units to be implemented utilizing simple rational expressions which provides a high level of security.

Elliptic curve cryptography is based on binary and primary field where we use it for key generation, encryption and decryption depending on the curve. It is an asymmetric key cryptography as different key is used for generating public key and private key. The public key is open to all but the private key is kept secret. ECC uses mathematical approach as compared to DH, RSA, ElGamal, and DSA. ECC is also used for digital signatures and key agreement. Today as more and more internet is used and for more security the large key size requirement is the necessity and at present RSA is using 1024 bit key size but it is not so sufficient for future use whereas the same level of security can be achieved from ECC using 160 bit key also which provide us the advantages [56][55] such as small key size, Absence of sub exponential time algorithm, less bandwidth, Faster implementation, Low computation cost, High speed, Low power consumption, Suitable for small scale size, Overloading is decreased.

For elliptic curve the dependency is on the domain parameters and the finite field Fp or F^{2m} can be selected. The security of ECC depends on the DLP problem i.e. Discrete Logarithm Problem, If P and Q are two points on any elliptic curve so that Q=kP,then it is easy to obtain Q when we know k and P but hard to know k even if we know P and Q as k should be large .this k is the DLP of Q to the base p and law of multiplication is used. If suppose P and Q is known then also at least square root of the number of the points on average to find k and if the field size if f^{2m} then at least $2^{(m/2)}$ points must be guessed to crack this.[13].Two method that are used for solving DLP are square root method and Silver-pohlig-Hellman, to avoid this use a large prime so that the facto also include large prime which will very exponentially, that why ECC provide a high level of security and RSA security is depended on the difficulty of factoring large numbers and it takes sub exponential amount to break.NIST had recommended that 1024 bits are sufficient for use until 2010.[57]

III. ELLIPTIC CURVE CRYPTOGRAPHY BASED APPROACHES

1. Identity Based Cryptography

In [3] Tate pairing is used for authentication and authorization of GSI. Use of non–interaction secret sharing protocol and one round tripartite DH protocol is done to propose PKG security infrastructure. ID based security infrastructure is compared with public key infrastructure and presented.

ID based authenticated multigroup keys agreement scheme is presented in [5] which use bilinear pairings. The users having different trust domains requires authentication and ID Based scheme provides mutual authentication for this using the shared password authentication mechanism for generating one time password for every session. The demerit of hash function compulsion in pairings based authentication protocol is been avoided using ID based authenticated multigroup keys agreement scheme and it is beneficial for large scale distributed and dynamic grid resources.

For efficient key management and moderate security a new scheme ID based proxy signature scheme is presented in [7].The ID based proxy signature scheme uses bilinear pairings. The proposed methodology is observed to be closely related to Diffie-Hellman of the random oracle model.

For secure resource allocation and to authenticate identities of grid members public key infrastructure (PKI) is used. For better security in grid security architecture Identity based cryptography is proposed in [9] which uses customized identity based key agreement protocol. This protocol provides more security and supports the delegation services and single sign on in GSI.

In grid computing security is an important issue .For more security user authentication scheme is developed in [16] which provides strong mutual authentication for user and server and requires only one way hash function and server private key.

Several issues related to Identity based using Tate pairing and Weil pairing has been discussed to increase the efficiency of the protocols. Authenticated key agreement (AK) protocol and AK with key confirmation (AKC) protocols is developed in [17] doing some changes in smart's AK protocol. This protocol avoids the key escrow of trust authority which issue private key and increase the benefits that is forward secrecy property.

A new protocol is presented in [18] using signature scheme based on bilinear pairings is identity based authenticated key agreement protocol which increases the efficiency and security of the two party authentications.

Proxy signature is being discussed today for much application such as distributed system and grid computing and some identity based proxy signature scheme are presented in concurrent years but they are not so efficient when we talk about security and computation. A more secure identity based strong designated verifier proxy signature (ID-SDVPS) based on elliptic curve bilinear pairings in [19] for more security is presented. The proposed scheme is suitable where more security and less computational cost requirement is such as in grid computing.

In [20] for scalar multiplication a new algorithm is proposed which is faster and based on Tate pairings using the elliptic curve over F_{2m}. By this technique speed is being improved and this is evaluated comparing it to RSA.

Paring based cryptosystems is mainly based on identity based encryption which provides security in improved way. Tate pairing in [21] is used to show the operations using the different co-ordinates of elliptic curve to improve the performance of pairings.

Bilinear maps based on wail pairings is used and a new identity based encryption is discussed in [23] using the random oracle model security and their applications for system which required security.

In [25] a new Hierarchical identity based encryption (HIBE) is presented which provide full security in random oracle model based on bilinear pairings.

Based on bilinear pairings where only two bilinear map computations is required for cipher text, HIBE is proposed in [26] which provide efficiency and short cipher text with secure public key and fully secure in random oracle model and also limited delegation is supported.

Without using random oracle model a new anonymous hierarchical identity based encryption is developed in [27] which reduce the computation cost as no dependency on the depth of hierarchy. The scheme is based on composite bilinear group which acquires selective-ID security.

Use of Identity based cryptography is discussed in [28] for Grid security architecture to improve the computational power and scalability.

Extensive use of public key certificates for long term and short term in PKI is replaced using IBC in [29].IBC provides more security, lightweight in grid with simple way when compared with conventional PKI.

For identity based cryptography a distributed (PKG) is proposed in [30] to overcome the problem of key escrow using the bilinear pairings and proved under the random oracle model and analysis is also done.

Using the property of identity based cryptography a new concept is developed in [31] that is dynamic key infrastructure for grid which introduce the concept of master public key to compute per session key by any user.

For cloud security a new architecture is discussed in [33] using the combination of Identity based encryption and identity

based signatures with an authentication protocol providing efficiency and reducing the computational cost.

Different properties of pairing are discussed in [34] when used in cryptography and to compare the pairings and the easy way of pairing to be used to design in the cryptographic schemes in grid architecture.

Using the concept of identity based cryptography a new method of generating public keys is presented in [35] that is identity based secret public keys using random strings which provides more security against online passwords guessing and other attacks when compared with RSA or DH. The protocol also allow secure establishment of TLS channels with allow passwords.

X.509 certificates and PKI are mostly used for grid authentication but include some demerits such as low anti-attack capability with poor efficiency. To improve this identity based cryptography is discussed in [37] for secure end efficient grid authentication without using random oracles and the proposed method is used to create private keys.

In[48] Enhanced Identity based cryptography(EIBC) for key management is discussed and is based on identity based cryptography which provide an easy way to manage keys and increasing the efficiency providing high level of security for smart grid networks.

2. Certificateless Based Cryptography

Some application of bilinear pairings are: - (i) signatures scheme (ii) pairing based encryption schemes or others are presented. A Certificateless signature based scheme is proposed in [6] which uses bilinear pairing. It does not involve pairing computation, also certificateless proxy signature scheme is proposed and both schemes are analyzed from point of security.

In [11] certificateless protocol for authentication and key agreement (CL-AK) is proposed for grid computing. Some benefits proved of the proposed protocol are: - efficiency, forward secrecy, known key secrecy and no key control.

In open network data encryption is mostly used and for this purpose RSA and DH are used mostly, but it is not much suitable for large number of bits.

To overcome the problem of RSA and Diffie Hellman. ECC is used in [12] for encryption /decryption of a text message by transforming the message on the elliptic curve over GF (p) using the point Pm(x, y).

Certificate-less public key cryptography avoids key escrow problem of identity based cryptography and more security in grid security infrastructure .In this without pairings the certificateless is proposed [36] which eliminates the type-I attack.

For authentication of identity, identity based cryptography uses certificates which increases overhead. to reduce this overhead a new scheme is proposed in [38].This scheme is certificateless based on elliptic curves named Elliptic curve based certificateless signatures for identity based encryption(ECCSI) which has some advantages such as low computation and low bandwidth.

With the use of certificateless public key cryptography use of certificates has been tried to removed in[45] to generate private and public key for the user.

In [46] a new certificateless public key encryption (CLPKE) is developed which is bilinear free and proved under random oracle model. This encryption scheme is more secure against ciphertext attack, key replacement attack and more.

Certificateless key agreement is mostly done using the bilinear pairings which increases the computational cost but here a new authenticated key protocol is used in[47] which is based on certificateless and does not require bilinear pairings which reduce the cost and provide more efficiency.

A new secure and efficient certificateless two party authenticated key agreement protocols (CTAKA) is proposed in [49]. The protocol is secure against Type-I and Type-II attacks. Pairing is not used which reduces the computational cost with no requirement of interaction between the communicating parties.

To avoid the key escrow problem of identity based, certificateless key agreement is used which improve the performance as discussed in [50].

Using bilinear parings certificateless authenticate key agreement protocol is revised in [51] which is also proved secure under random oracle model.

Construction of certificateless key agreement protocol is done in [58] from the certificateless key encapsulation which provide more security from Type-I and Type-II attacks in the CK model.

A new key generation technique is discussed in [59] for private key and public key using certificateless public key cryptography which can produce multiple public keys for a single private key increasing the security.

Certificateless public key cryptography has the combined features of identity based and PKI and a new certificateless two party key agreement protocol has been proposed in [60] two show that it is more practical when compared with others.

Pairing free protocols has been developed in [61] to show that they are more secure in random oracle model using elliptic curves with certificateless key agreement protocol.

In any open network key agreement is an important process which should be authenticated to avoid active attacks and for this Simulatable certificateless two party protocol has been discussed in [62].

3. Others

Elliptic curve cryptography is the best algorithm for solving the elliptic curve discrete logarithm problem used in [1] when compared to RSA, with small parameters and providing more security with the small key size. Some benefits of ECC are:

(i) Key exchange (ii) key generation (iii) digital signature.

In [2] a new scheme named ECGSC is proposed based upon ECDSA and Generalized Signcryption. Confidentiality, Non-repudiation and Unforgeability are proven based on Random Oracle Model.ECGSC increases the security with low computational cost with 78%.

For secure digital images an efficient symmetric encryption is proposed in [4] which reduces the disadvantages of system performance, security and small key space problem and based on cyclic elliptic curve and chaotic system. With eight 32bit registers it converts the 256 bit plain image into 256 bit of cipher image generating pseudorandom bit sequence for round keys. This scheme increases the security of the images and fast encryption is done as compared to others.

Security in wireless channels requires: - (i) encryption (ii) authentication (iii) authorization. When communicating over

public network as web some factor to be considered are privacy and anonymity .In [8] ECC is used to extend onion routing for dynamic token exchange.ECC provides better results in terms of memory, smaller key size, faster computation, bandwidth savings, low power consumption and faster computation as compared to Rascals the performance of both ECC and RSA has been compared

Some security threats and attacks in grid networks are: - eavesdropping, impersonation and message modification etc. Robust and efficient authentication protocol is presented in[10] using ECC to enhance the security in grid networks which also allow mutual authentication and session key agreement increasing the security such as session key security and known key security.

Password Authenticated Key Exchange (PAKE) protocol is being proposed in [14] with ECC approach. The proposed protocol is implemented in two steps:

(I)An auxiliary mechanism (ECC version of PAKE) is proposed

(ii)Extend the mechanism to a multilayer consensus model.

The benefits of the proposed protocol is that hash function is reduced to one and password shared id being utilized in home area network controller for smart grid and only 12 packets is required to exchange which reduce the delay by one and a half.

In [15] pairing based cryptography is presented using some application of bilinear pairings which provide some mechanism for trust delegation and confidentiality for grid computing.

The problem of poor scalability in GSI architecture due to GSI authentication arising when using the security protocols. In [22] to improve the scalability problem a new authentication framework using bilinear pairings is presented which help to minimize the frequent communications.

For grid application a new authentication is discussed in [24] where passwords are used to authenticate the users supporting mutual authentication, delegation without certificates.

In [32] RSA and ECC are compared where ECC is used now days as an alternative solution increasing scalability, efficiency and performance in GSI.

Use of elliptic curve in elliptic curve cryptography helps to reduce the modular exponentiation .based on this a new method is introduced in [39] which offers private credentials .this helps to reduce property sharing resistance. Unforgeability etc.

A relationship between mathematics and cryptography is discussed in [40] related to the context of elliptic curve which intractable when we talk about complexity. In these biometric signatures is presented which provide high speed and high security.

A discussion about elliptic curve cryptography is done in [41] with a comparison of RSA that how it can be used in network security .Benefits of ECC when compared to RSA is that is provide high speed and more security with smaller keys.

In [42] elliptic curve is applied and a new pairing method is introduced which is pairing based remote authentication. In this method no requirement of password of the login user and they can change their password when they want. Increasing the flexibility of the authentication scheme.

Using elliptic curve cryptography a new access control scheme is proposed in [43] to reduce the security problems as compared to public key-based access control.

To secure elliptic curve cryptosystems, new algorithm is presented fractional width-want is presented in [44] to resist some attacks as side channel attacks. The algorithm reduces the computation cost at lowest.

IV. CONCLUSION

Use of identity based and certificateless based key agreement using elliptic curve cryptography are today's most important techniques used to increase the distributed system security and this techniques has replaced the traditional PKI, it has reduced the more consumption of power bandwidth ,less costs and small key size providing more security. Certificateless based public key cryptography has eliminated the need of certificate required for key distribution. No key escrow problem that occurs in ID based, Partial private key is generated so no breaching of private key, Increased efficiency, Reduced cost, Use of the technology is simple. When requirement of short term private key generation ID based is suitable but when long term is required use of certificate-less is better option. With or without bilinear pairing certificateless and ID based is used as it is required. Comparison of these are given in table II.

Features	Public key cryptography	Identity based cryptography	Certificateless based cryptography
Private key creation	By the use of certificates	Using the trusted authority	Partial private key is generated using KGC and other is generated by the user.
Public Key generation	By the use of certificates	Using the user's identity	No public key certificate is used
Trust	Trust problems is there	Trust management takes place	Updation of trust in after every session
Authenticity	Certificate demonstrates the authentication of identifying information	Public key is generated before generation of private key so trusted authority need not to authenticate	Partial key is generated so no requirement of authenticity
Identity based	Yes	Yes	No

Table II Comparison among PKI,ID based, Certificateless based.

REFERENCES

[1] Y.Zhu, X.Lin and G.Wang, "Design of Elliptic Curve Cryptography in GSI", International conference on high performance computing and application, 2005, pp.623-628.

[2] Y.Han, X.Y., Ping W., Y.Wang and Y. Hu, "ECGSC: Elliptic Curve Based Generalized Signcryption", lecture notes in computer science Volume 4159, 2006, pp. 956-965.

[3] X. Huang,L. Chen,L. Huang and M. Li , "An Identity-Based Model for Grid Security Infrastructure", Lecture Notes in Computer Science Volume 3563,2005, pp. 258-266.

[4] A. Abd El-Latif, Li and X. Niu , "A new image encryption scheme based on cyclic elliptic curve and chaotic system", 2008 International Symposium on Electronic Commerce and Security, july 2012.

[5] X.wang and S.wang, "ID based Authenticated multigroup keys agreement scheme for grid computing", vol 6320, 2010, pp. 259-266.

[6] X.lin, k.chen and l.sun, "certificateless signature and proxy signature schemes from bilinear parings", vol 45.issue 1, 2005, pp. 76-83.

[7] J.Xu, Z. Zhang and D.feng, "ID based proxy signature using bilinear pairings", vol 3759, 2005, pp. 359-367.

[8] H. P. Begam and M. Mohamed , "Performance Analysis of Elliptic Curve Cryptography Using Onion Routing to Enhance the Privacy and Anonymity in Grid Computing", International Journal of Future Computer and Communication, vol. 1, No. 2, August 2012.

[9] H.W.lim and K.G.Paterson, "Identity based cryptography for grid security", international journal of information security, vol 10, feb 2011, pp. 15-32,.

[10] L.zhang, Wuhan, S.tang, Y.jiang and Z.Ma, "Robust and efficient authentication protocol based on elliptic curve cryptography for smart grids", IEEE international conference, Aug 2013, pp. 2089-2093.

[11] S.Wang1, Z.cao and H.bao, "Efficient certificateless authentication and key agreement for grid computing", International journal of network security, vol 7, no.3, Nov 2008, pp. 342-347.

[12] S.Vigila, N.islam, and K.Muneeswaran, "Implementation of text based cryptosytem using elliptic curve cryptography", first international conference on advance computing , Dec 2009, pp. 82-85

[13] T.N.Shankar and G.sahoo, Cryptography with Elliptic curves, International Journal of Computer and Application Vol2, May 2009 .

[14] H. Nicanfar and V.C.M.leung "Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) Protocol for Smart Grid System", Volume: 4, Issue: 1, Mar 2013, pp.253 - 264.

[15] A.Saxena, La Trobe, Bundoora and B.Soh, "Pairing Based Cryptography for Distributed and Grid computing", IEEE international conference on communications, Vol 5, June 2006, pp.2335 - 2339.

[16] R.Lu, Z. Cao, Z. Chai, and X.i Liang and R. lu, "A Simple User Authentication Scheme for Grid Computing", International Journal of Network Security, Vol.7, No.2, Sept. 2008, pp .202–206

[17] L. Chen and C. Kudla, "Identity Based Authenticated Key Agreement Protocols from Pairings", 16thIEEE Computer security foundation, July 2003, pp.219-233.

[18] Marko Hölbl,Tatjana Welzer,Boštjan Brumen, "An improved two-party identity-based authenticated key agreement protocol using pairings", Journal of Computer and System Sciences, Vol 78, Issue 1, January 2012, pp. 142–150.

[19] SK Hafizul Islam,and G.P. Biswas, "A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings", Journal of King Saud University - Computer and Information Sciences, Vol 26, Issue 1, January 2014, pp. 55–67.

[20] P.S.L.M Barreto, H.Y.Lim, B.Lynn and M.scott. "Efficient algorithms for pairings based cryptosystems.", In m.Yung editor, advances in cryptology-proceedings of crypto 2002, and springer Verlag LNCS 2442, 2002, pp. 354-368.

[21] Z.Cheng and M.Nistszakis, "Impelementing Pairing Based cryptosystems", 2005

[22] L.Chen, H.W.Lim and W.Mao, "User-friendly Grid Security Architecture and protocols", Lecture notes in computer science, vol 4631,2007, pp. 139-156.

[23] Debone, M.Frankliny, "Identity-Based From Weil Pairing", lecture notes in computer science, Proceedings of crypto 2001, vol 2139, 2001, pp.213-229, springer Verlag.

[24] J.crampton, H.W.Lim, K.G.Paterson and G.Price, "A certificate- free grid security infrastructure supporting password based user authentication", in proceedings of 6th annual PKI R&D workshop, 2007.

[25] C.Gentryl and A.silverberg, " Hierarchical ID based cryptography", In Y.Zheng,editor,Advances in cryptology-proceedings of ASIACRYPT 2002, Springer Verlag, pp.548-566.

[26] D.Boneh, X.Boyen and Eu-Jin Goh, "Hierarchical identity based encryption with constant size cipher text", Advances in cryptology-EUROCRYPT 2005, vol 3493, lecture notes in computer science, springer, 2005, pp. 440-456.

[27] J.Hong Seo, T.Kobayashi, M.Ohkubu and K. Suzuki, "Anonymous Hierarchical Identity-Based encryption with constant size ciphertexts", Lecture notes in computer science, vol5543, 2009, pp. 215-234.

[28] H.W.Lim and M.J.B.Robshaw, "On identity-based cryptography and grid computing", lecture notes in computer science, Proceedings off the 4th international conference on computational science (ICCS 2004), vol-3036, 2004, pp. 474-477.

[29] H.W.Lim, "Designing grid security infrastructure using Identity based cryptography", 2010.

[30] A.Kate and I.Golberg, "Distributed Private-key generators for identity-based cryptography",2009.

[31] H.W.Lim and M.J.B. Robshaw, "A dynamic infrastructure for grid", proceedings of the European grid conference (EGC 2005) , 2005, pp. 255-264, Springer Verlag LNCS 3470.

[32] H.Khurana, R.Koleva and J.Basney, "Performance of cryptographic protocols for high-performance, high-bandwidth and high-latency grid systems", IEEE international conference on e science and grid computing, dec 2007, pp. 431-439.

[33] H.Li, D.Yuanshun and B.Yang, "Identity based cryptography for cloud security", IACR Cryptology ePrint Archive 01/2011; 2011.

[34] S.D.Galbraith, K.G.Paterson and N.P.smart, "Pairings for cryptographers", 2008.

[35] M.Hedayati, S.H.kamali and R.Shakerian, "Using Identity-based public keys cryptography for heuristic security analyses in grid computing", 2010.

[36] G.sharma, S.bal and A.K. Verma, "On the security of certificateless signature schemes", international journal of distributed sensor networks, 2013.

[37] Z.Yan, H.Wang, R.Wang, "Grid authentication from identity-based cryptography without random oracles", Journal of posts and telecommunications, Dec 2008.

[38] M.groves, "Elliptic curve-based certificateless signatures for identity based encryption (ECCSI)", Feb 2012.

[39] [39] A.athavale, K.singh and Sasswood, "Design of a private credentials scheme based on elliptic curve cryptography", first international conference on computational intelligence, communication systems and networks, July 2009, pp332-335.

[40] O.S.Althobaiti and H.A. Aboalsamh, "An enhanced elliptic curve cryptography for biometric", 7th International conference on computing and convergence technology (ICCCT) , Dec 2012, pp. 1048-1055.

[41] M.Amara and A.Siad, "Elliptic curve cryptography and its application", International conference on systems, signal processing and their applications (WOSSPA) , May2011, pp. 247-250.

[42] W.T.Shvi, J.H.Chiu and B.C.Chieu, "ID based remote authentication with smart cards on open distributed system from elliptic curve cryptography", IEEE conference on Electro Information Technology, May 2005.

[43] X.H.Le,S.Lee,I.Butun and M.Khalid, " An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography", Journal of communications and networks, vol11,issue6,Dec2009, pp. 599-606.

[44] T.Zhang, F.Mingyu and X.Zheng, "secure and efficient elliptic curve cryptography resists side channel attacks", journal of systems enginnering and electronics, vol20, issue3, June 2005, pp. 660-665.

[45] A.Sarkar and S. Tripathi, "Removal of certificates from set protocol using certificateless public key cryptography", International Journal of Network Security and Application,2012.

[46] AJ.Back,R.S.Nain and W.Susilo, "certifcateless public key encryption without pairings",2006.

[47] Y.J.kim,Y.m.Kim,Y.J.Choel and H.Chol, "An efficient bilinear pairing free certificateless two party authenticated key agreement protocol in the eCK model", june 2013.

[48] H.Nicanfar and V.C.M.Leung, "EIBC:enhanced identity-based cryptography, a conceptual design", IEEE international conference on systems conference(sysCon) ,March 2012 ,pp. 1-7.

[49] N.A.F.Mohamed, M.H.A.Hashim, E.B.M Bashier and M.E.H Hassouna, " Fully-secure and efficient pairing-free cretificateless authenticated key agreement protocol", Internet security,June2012, pp. 167-172.

[50] D.He and Y.Chen, "An Efficient certificteless authenticated key agreement protocol without bilinear pairings",2011.

[51] D.Goya,C.Okida and R.Terada, "A two party certificateless authenticated key agreement protocol,2010.

[52] Koblitz N, Menezes A.J and Vanstone S.A, "The state of elliptic curve cryptography".Design Codes and Cryptography.Vol 19, Issue 2-3, 2000.

[53] Miller V. "Use of elliptic curves in cryptography." Advances in Cryptography-Crypto '85. LNCS 218, Springer Verlag, 1986, 417-426.Silverman, The Arithmetic of Elliptic curves, Springer-Verlag, New York, 1986.

[54] J.W.Bos, A.Halderman, N.Heninger, J.Moore, M.Naehrig and E.Wustrow, Elliptic curve Cryptography in practice, 2013.

[55] R.Shanmugalakshmi, M. Prabhu, "Research Issues on Elliptic curve Cryptography and its application", IJCSNS Intenational Journal of Computer Science and network Security, 2009.

[56] L.Tutanescu, "Application of Elliptic curve Cryptosystems", MCC Coference proceedings, Bonn, Germany, 2007.

[57] I.Tutanescu, C.Anton and D. Caragata, "Use of Elliptic Curve Cryptography in Information Security", ICIT the 5th international Conference on Information Technology, 2011.

[58] G.Lippold,j.G.Nieto, "Certificateless key agreement in the standard model",2010.

[59] S.R.Chunamari and D.G. Borse "Robust framework for certifcateless authneticated key agreement protocol", International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012) Proceedings published in International Journal of Computer Applications(IJCA) (0975 – 8887) 27 ,2012.

[60] Y.Ying, H.Ke and Z.Wnefang, "An efficient ccertificateless authenticated key agreemtent", Journal of theoretical and applied infromation technology,2013.

[61] Z.Zhu "cryptanalysis of pairing free certificateless authenticated key agreement protocol", International Journal of Communcation system, 2012,pp. 221-230.

[62] L.Zhang, " Simulatable certificateless two party authenticated key agreement protocol",2009.

AUTHORS

First Author – Garima Verma,MTech 2nd Year,Babu Banarasi das University,email id-garimaverma964@gmail.com
Second Author – Amandeep Kaur, MTech,Babu Banarasi das University,email id- er.amandeep.kaur3@gmail.com