A TAXONOMY AND COMPARISON OF TWO-PARTY KEY AGREEMENT PROTOCOLS

Ch. Asha Jyothi[1], G. Narsimha[2], J.Prathap[3]

[1]*Dept. of Information Technology, JNTUHCEJ, Karimnagar, Telangana, India*
[2]*Dept. of Computer Science and Engg, JNTUHCEJ, Karimnagar, Telangana, India*
[3]*Dept. of Computer Science and Engg, Sree Chaitanya College of Engineering, Karimnagar, Telangana, India*

Abstract

Key Management in symmetric cryptography is to securely share a secret key between the two communicating individuals. The popular solution to this key management issue is to use public key cryptography schemes. The key management techniques are broadly classified into Key Distribution protocols and Key Agreement protocols. This paper presents the detailed classification of Key Agreement protocols and provides some of the existing ECC based protocols in each category. Recently much work has been carried out in Identity Based Cryptography IBC, Certificateless Public Key Cryptography CLPKC and Pairing Based Cryptography PBC based techniques for key agreement. This paper also presents the comparison of two-party key agreement protocols under these areas based on the computational cost calculated in the key agreement phase.

Keywords *– Key Management, Key Agreement, Public Key Infrastructure, Identity Based Cryptography, Certificateless Public Key Cryptography, Pairing Based Cryptography.*

----------***----------

1. INTRODUCTION

A Key establishment [1] protocol permits two or more parties to gain access to a shared secret key. These protocols can be divided into two categories namely key distribution protocols and key agreement protocols. Key distribution protocols allow any one user to choose the secret key and distribute it secretly to the other parties. In Key agreement protocols, the shared secret is a function of the information or values provided by every user. In other words, Key agreement protocols allow two or more parties to derive the shared secret key from the information provided by each of the party. Key agreement protocols can further be divided into two-party or peer-to-peer key agreement protocols and Group key agreement protocols. This paper presents the survey on the two-party key agreement protocols.

The secret key shared using the two-party key agreement protocols can further be used to exchange the messages confidentially with the help of any symmetric cryptographic algorithms. Previous to any secured communication with symmetric cryptography [2], users must set up a secret key between the two ends of communication. The progress of public key cryptography in the 1970s has made the sharing of secret keys less worrying. From the time when the Diffie-Hellman key exchange protocol published in 1975, it has become possible to securely exchange a secret key and has significantly reduced the danger of key disclosure during the establishment of a secret key. On the basis of existing algorithms in literature, the public key cryptography solutions for secret key agreement can be classified into four categories: Public Key Infrastructure PKI, Identity Based Cryptography IBC, Certificateless Public Key Cryptography CLPKC and Pairing Based Cryptography PBC.

Traditional PKI techniques [3] for key agreement need a public key certificate to ensure the relation between a public key and the identity of the holder. These techniques suffer from the cumbersome certificate management with the certification authority hierarchy. In IBC, a user's public key can be derived from his identity (name or email address) and his private key is created by a trusted third party called the key generation center (KGC) by binding the identity of the user with his master-key. IBC [4] suffers from key escrow problem because not only the user but KGC also knows the users private key. If KGC is compromised then the entire user's (registered under that KGC) private keys are disclosed to the unauthorized users. CLPKC resolves the key escrow problem in IBC by allowing KGC to generate only partial private key and the user will generate the full private key using the partial private key and some secret value chosen by him. IBC techniques for key agreement can further be divided into pairing-based IBC and pairing-free IBC. Pairing based IBC involves the use of bilinear maps or pairings that are computationally intensive. Pairing-free IBC does not involve the use of pairings but involves normal elliptic curve point arithmetic. There are also key agreement techniques that involve only pairing based cryptography without using IBC or CLPKC. The above presented classification or taxonomy is pictorially represented in Fig 1. The algorithms under the given classifications during the past recent decade are studied in this paper.

All the PKI, IBC and CLPKC techniques involve the use of central authority say PKI uses Certification Authority CA, IBC and CLPKC uses Key Generation Centre KGC. Key agreement techniques that solely use PBC can be classified into those that need central authority (Central Authority Based) and those that do not need central authority (Central Authority Free).

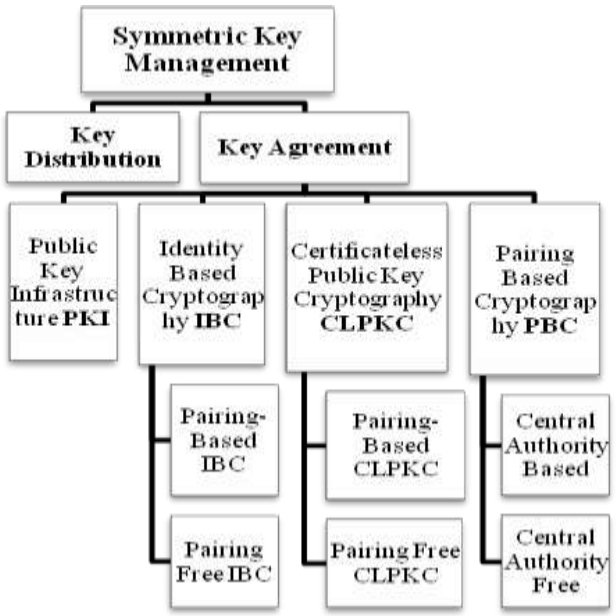

Fig 1. Classification of Key Management techniques

All the traditional public key cryptography solutions prior to IBC are related to PKI techniques for key agreement like RSA, Diffie-Hellman key exchange protocols, ECC based key exchange protocols. Recently much work has been carried out on IBC, CLPKC and PBC based techniques for key agreement. So here we present the comparison of protocols under IBC, CLPKC and PBC categories. These techniques are special case of Elliptic Curve Cryptography as they involve computations on elliptic curve points. The mathematical backgrounds needed by these protocols are elliptic curve cryptography and bilinear maps or pairings.

The paper is organized as Section II presents the mathematical backgrounds needed for the various two-party key agreement protocols. Section III presents one of the categories of key agreement protocols namely Cetificateless Public key Cryptography protocols. Section IV presents another category of key agreement protocols namely Identity based Cryptography protocols. Section V presents one more kind of key agreement protocols namely Pairing Based Cryptography protocols. Section VI presents the Conclusion that gives the summary of the paper.

2. MATHEMATICAL BACKGROUND

As per the classification said above, the various categories of two-party key agreement protocols are based on either elliptic curve cryptography or pairings. Hence this section presents them in brief.

2.1 Elliptic Curve Cryptography

An elliptic curve E over a field K is a set of points (x, y) with x, y ∈ K, together with a special point **O** called the point at infinity. The (x, y) points are the roots of a Weierstrauss equation of the form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

For a particular field K, the Weierstrauss equation takes a simpler form $y^2 = x^3 + ax + b$. In cryptography the special elliptic curves that are of interest are non-singular elliptic curves that must satisfy the necessary and sufficient condition $4a^3 + 27b^2 \neq 0$.

ECC depends on the hardness of the discrete logarithm problem. Let P and Q be two points on an elliptic curve such that kP = Q, where k is a scalar. Given P and Q, it is hard to compute k. k is the discrete logarithm of Q to the base P.

Elliptic curve parameters over the finite field F_p is a tuple T = <q, E, a, b, G, n, h>, where

- q = the prime p
- a, b: the curve coefficients
- G: the base point (G_x, G_y)
- n: the order of G
- h: $\#E(F_q)/n$.
- E: $y^2 = x^3 + ax + b$

$$E(F_q) = \{(x, y) \in E : y^2 = x^3 + ax + b \setminus x,y \in F_q\} \cup \{\mathbf{O}\}$$

The main operation most commonly used in cryptographic protocols is point multiplication with a scalar. Multiplication of k * P to achieve another point Q is treated as P added to itself for k times, that is k * P = Q = P + P +… + P (k times).

2.2 Bilinear maps or Pairings

Consider two additively written abelian groups A_1 and A_2; the identity element being 0. Also consider a multiplicatively written cyclic group C; the identity element being 1. A pairing on A_1 , A_2 and C is a non-degenerate, bilinear map e such that

$$e : A_1 \times A_2 \rightarrow C.$$

A bilinear pairing or just pairing e is a function which maps a pair of points on an elliptic curve E, defined over fields A_1 and A_2, to an element of the multiplicative group of a finite extension field C. This mapping is said to be bilinear pairing as it maps a pair of elliptic curve points. The pairing e has the following characteristics:

Non-degenerate: Given a point $\mathbf{O} \neq X \in A_1$ there is a point $Y \in A_2$ such that $e(X, Y) \neq 1$; where **O** is the point at infinity on the elliptic curve over the finite field A_1 and A_2.

Bilinear: for all points $X, X_1, X_2 \in A_1$, and $Y, Y_1, Y_2 \in A_2$ and scalars $u, v \in Z$ we have

$$e(X_1 + X_2, Y_1) = e(X_1, Y_1)\, e(X_2, Y_1),$$

$$e(X_1, Y_1 + Y_2) = e(X_1, Y_1)\, e(X_1, Y_2).$$

This can be redefined in the following way:

$$e([u]X, [v]Y) = e(X, Y)^{uv} = e([v]X, [u]Y); \text{ where } [u]X = u * X = X + X +..+ X \text{ (u times)}$$

Computable: There exists a computationally efficient algorithm to find e(X, Y) for all $X \in A_1$ and $Y \in A_2$.

3. CERTIFICATELESS PUBLIC KEY CRYPTOGRAPHY CLPKC PROTOCOLS

CLPKC protocols (both Pairing Based and Pairing Free) have six algorithms [6][15]: "Setup, Partial Private Key Extract, Set Secret Value, Set Private Key, Set Public Key and Key Agreement." *Setup algorithm* is used by KGC to generate the system public parameters and the master key. These system parameters are input to all subsequent algorithms. KGC uses *Partial Private Key Extract algorithm* to generate partial private key from the user's identity and his master key. The user uses *Set Secret Value algorithm* to generate the secret value from his ID. The user uses *Set Private Key algorithm* to generate the complete private key from the partial private key and secret value. The user uses *Set Public Key algorithm* to generate the public key from the secret value and his ID. *Key agreement algorithm* is an interactive protocol between the two users that uses all the values generated in previous algorithms and allows to share a common secret key. The comparisons of protocols shown in all tables involve only the operations done in the key agreement phase but not including all the earlier phases. From the Table 1, Seyed-Mohsen Ghoreishi [26] protocol is efficient in computational cost. From Table 2, WANG Shengbao et. al. [22] protocol is efficient in computational cost. The time factors involved in framing the computational cost are as follows:

- T_{spmul} : The time taken for scalar point multiplication.
- T_{ppmul} : The time taken for point-point multiplication
- T_{padd} : The time taken for point addition.
- T_{hash} : The time taken for hash function.
- T_{sinv} : The time taken for scalar inversion.
- T_{pinv} : The time taken for point inversion.
- T_{pair} : The time taken for pairing.
- T_{exp} : The time taken for point exponentiation.
- T_{mexp} : The time taken for modular exponentiation.
- T_{mac} : The time taken for MAC algorithm.
- T_{ppdiv} : The time taken for point-point division.

Table 1 Computational comparison of various Pairing Free CLPKC protocols

Protocol	Computational Cost
Yasmine Abouelseoud [13]	$3\ T_{spmul} + 3\ T_{padd} + 2T_{hash}$
Amr Farouk [11]	$3\ T_{spmul} + 5\ T_{padd} + 2\ T_{hash}$
Debiao He [3]	$5\ T_{spmul} + 3\ T_{padd} + 2\ T_{hash}$
He Debiao [7]	$5T_{spmul} + 3\ T_{padd} + 2\ T_{hash} + 1\ T_{sinv}$
He Debiao [8]	$5\ T_{spmul} + 4\ T_{padd} + 2\ T_{hash}$
G. Yang [9]	$9\ T_{spmul} + 2\ T_{hash}$
Mengbo Hou [10]	$6\ T_{spmul} + 2\ T_{hash}$
Manman Geng [6]	$7\ T_{spmul} + 2\ T_{hash}$
S-M Ghoreishi [26]	$3\ T_{spmul} + 1\ T_{hash}$

Table 2 Computational comparison of various Pairing Based CLPKC protocols

Protocol	Computational Cost
Lei Zhang [12]	$2\ T_{pair} + 4\ T_{spmul} + 2\ T_{hash}$
LI Gui-ying [14]	$2\ T_{pair} + 5\ T_{spmul} + 4\ T_{padd} + 1\ T_{hash}$
Lei Zhang [15]	$2\ T_{pair} + 4\ T_{spmul} + 2\ T_{hash}$
PAN Jin [16]	$2\ T_{pair} + 2\ T_{spmul} + 1\ T_{padd} + 2\ T_{hash}$
Lei Zhang [17]	$1\ T_{pair} + 4\ T_{spmul} + 2\ T_{padd} + 2\ T_{hash}$
Liu Wenhao [18]	$2\ T_{pair} + 2\ T_{spmul} + 2\ T_{hash}$
Mengbo Hou [19]	$1\ T_{pair} + 1\ T_{exp} + 4\ T_{spmul} + 1\ T_{padd} + 1\ T_{hash}$
Tarjei K. Mandt [20]	$2\ T_{pair} + 1\ T_{exp} + 3\ T_{spmul} + 2\ T_{padd} + 1\ T_{mac}$
SHI Yijuan [21]	$1\ T_{pair} + 1\ T_{exp} + 2\ T_{spmul} + 1\ T_{padd} + 1\ T_{hash}$
WANG Shengbao [22]	$1\ T_{pair} + 3\ T_{spmul} + T_{hash}$

4. IDENTITY BASED CRYPTOGRAPHY IBC PROTOCOLS

Most of the IBC based protocols make use of bilinear pairings and these protocols are termed as Pairing Based IBC systems as per the above given classification. To solve the troubles due to the bilinear pairings [23], IBC systems based on elliptic curves have been initiated and explored in various security related areas together with key agreement protocols. These systems under the above given classification can be termed as Pairing Free IBC systems. These protocols (both Pairing Based and Pairing Free) have three phases [24]: "Setup, Extract and Key Agreement." *Setup phase* executed by KGC, will generate the system parameters and master key from a given security parameter. *Extract phase* executed by KGC, takes system parameters, master key, and a user's identifier as input and returns the user's private long-term key. *Key agreement phase* is used by users to establish a common secret key among them. From Table 3, Xuefei Cao et al. [24], Robert W. Zhu et al. [25] are efficient in computational cost. From Table 4, Takeshi Okamoto et al. [30] protocol scheme II is efficient in computational cost.

Table 3 Computational comparison of various Pairing Free IBC protocols

Protocol	Computational Cost
M S Farash [23]	8 Tspmul + 1 Tpadd + 2 Thash
Xuefei Cao [24]	5 Tpsmul + 2 Tpadd + 2 Thash
Robert W. Zhu [25]	5 Tpsmul + 2 Tpadd + 2Thash

Table 4 Computational comparison of various Pairing Based IBC protocols

Protocol	Computational Cost
Quan Yuan [5]	$1\ T_{pair} + 3\ T_{spmul} + 2\ T_{padd} + 1\ T_{hash}$
Xiufeng Zhao [27]	$3\ T_{pair} + 4\ T_{exp}$
Liang Ni [28]	$5\ T_{pair} + 1\ T_{exp} + 4\ T_{spmul} + 1\ T_{hash}$

Hua Guo [29]	6 T_{pair} + 1 T_{ppdiv} + 6 T_{exp} + 1 T_{pinv}
Takeshi Okamoto [30]	Scheme I. 2 T_{pair} + 1 T_{exp} + 1 T_{spmul} + 1 T_{hash} Scheme II. 1 T_{pair} + 3 T_{spmul} + 1 T_{hash}
Marko Hölbl [31]	3 T_{pair} + 2 T_{exp} + 3 T_{spmul} + T_{padd} + 3 T_{hash}
NI Liang [32]	7 T_{pair} + 2 T_{exp} + 3 T_{spmul} +2 T_{hash}

5. PAIRING BASED CRYPTOGRAPHY PBC PROTOCOLS

The above said protocols Pairing Based IBC and Pairing Based CLPKC also make use of pairings along with Identity Based Cryptography and Certificateless cryptography concepts respectively. But the PBC protocols solely use pairings without IBC or CLPKC concepts. Of course pairing or bilinear map operation is computationally more complex, several pairing friendly elliptic curves [38] like Barreto-Naehrig BN curves, MNT curves, Freeman curves are invented to reduce the computational complexity of pairing operations. Hence PBC area has been extensively used in today's research.

Table 5 Computational comparison of various Central Authority Based PBC protocols

Protocol	Computational Cost
Chu-Hsing Lin [33]	1 T_{pair} + 1 T_{exp} + 1 T_{spmul} + 2 T_{padd} + 2 T_{sinv}
Weijun Zhang [37]	2 T_{pair} + 2 T_{spmul}

Table 6 Computational comparison of various Central Authority Free PBC protocols

Protocol	Computational Cost
Minghui Zheng [34]	1 T_{pair} + 1 T_{exp} + 7 T_{spmul} + 5 T_{hash}
Ch. Asha Jyothi [35]	1 T_{pair} + 1T_{exp} + 1T_{spmul}
Ch. Asha Jyothi [36]	3 T_{pair} + 3 T_{exp} + 6 T_{spmul}
Hongtu Li [39]	1 T_{pair} + 4 T_{spmul} +2 T_{hash}

The central authority free PBC protocol in [36] requires variable number of pairing operations. The computational cost given in Table 6 for [36] assumes (3,5) as the value for (t, n) verifiable secret sharing, which is the most common pair of values chosen for (t, n) threshold secret sharing schemes.

6. CONCLUSION

Symmetric Key Management is to exchange a secret key between the two ends of communication. The public key cryptography solutions for symmetric key management are studied here in the form of various types of protocols like PKI, IBC, CLPKC and PBC. These protocols can be applicable to different types of scenarios or networks depending on the nature of environment that exist. For Example, as the nodes in Mobile Ad hoc Networks and Wireless Sensor networks depend on battery power, they require protocols that are efficient in computation and hence consume less power. This paper has presented the classification and comparison of various two-party key agreement protocols especially that make use of ECC-based public key cryptography or Pairings-based public key cryptography.

REFERENCES

[1]. Johann Van Der Merwe, Dawoud Dawoud, Stephen McDonald, "A Survey on Peer-to-Peer Key Management for Mobile Ad Hoc Networks," ACM Computing Surveys, Vol. 39, No. 1, Article 1, April 2007.

[2]. https://en.wikipedia.org/wiki/Key_management

[3]. Debiao He, Sahadeo Padhye, Jianhua Chen, "An efficient certificateless two-party authenticated key agreement protocol," Computers and Mathematics with Applications, 64 (2012), pp.1914–1926, Elsevier 2012.

[4]. SK Hafizul Islam, G. P. Biswas, "An improved pairing-free identity-based authenticated key agreement protocol based on ECC," International Conference on Communication Technology and System Design 2011, pp. 499 – 507, Elsevier 2011

[5]. Quan Yuan, Songping Li, "A New Efficient ID-Based Authenticated Key Agreement Protocol," IACR Cryptology ePrint Archive, 2005.

[6]. Manman Geng, Futai Zhang, "Provably Secure Certificateless Two-Party Authenticated Key Agreement Protocol without Pairing," International Conference on Computational Intelligence and Security, pp. 208-212, IEEE 2009.

[7]. He Debiao, Chen Jianhua, Hu Jin, "A Pairing-free Certificateless Authenticated Key Agreement Protocol," International Journal of Communication Systems 25(2), pp. 221-230, 2012.

[8]. D. He, Y. Chen, J. Chen, R.Zhang, W. Han, "A new two-round certificateless authenticated key agreement protocol without bilinear pairings," Mathematical and Computer Modeling, Vol. 54 pp. 3143-3152, 2011.

[9]. G. Yang, C.Tan, "Strongly Secure certificateless key exchange without pairing," 6th ACM Symposium on Information, Computer and Communications Security, pp. 71-79, 2011.

[10]. Mengbo Hou, Qiuliang Xu, "A Two-Party Certificateless Authenticated Key Agreement Protocol without Pairing," International Conference on Computer Science and Information Technology, pp. 412-416, IEEE 2009.

[11]. Amr Farouk, Ali Miri, Mohamed M. Fouad, Ahmed A. Abdelhafez, "Efficient Pairing-Free, Certificateless Two-Party Authenticated Key Agreement Protocol for Grid Computing," IEEE, 2014.

[12]. Lei Zhang, "Certificateless one-pass and two-party authenticated key agreement protocol and its extensions," Information Sciences, Elsevier 2014.

[13]. Yasmine Abouelseoud, "Efficient Certificateless One-Pass Key Agreement Protocols," Proceedings of the World Congress on Engineering and Computer Science 2014 Vol II WCECS 2014.

[14]. LI Gui-ying, HOU Meng-bo, ZHAO Chuan, XU Qiu-liang, "A Two-party Certificateless Authenticated Key

Agreement Protocol with provable security," Ninth International Conference on Computational Intelligence and Security, IEEE 2013.
[15]. Lei Zhang, "Provably Secure Certificateless One-Way and Two-Party Authenticated Key Agreement Protocol," ICISC 2012, LNCS 7839, pp. 217–230, Springer-Verlag 2013.
[16]. PAN Jin, LIU Xiaoqiong, XIE Minghui, LIU Qiong, "Certificateless-based two-party authenticated Key agreement Protocols in a Multiple PKG Environment," International Conference on Computer Science and Network Technology, IEEE, Dec 2011.
[17]. Lei Zhang, Futai Zhang, Qianhong Wua, Josep Domingo-Ferrer, "Simulatable certificateless two-party authenticated key agreement protocol," Information Sciences Vol. 180 pp. 1020–1030, Elsevier 2010.
[18]. Liu Wenhao, Xu Chunxiang, Xu Jian, "Certificateless Two Party Key Agreement Protocol," International Conference on Multimedia Information Networking and Security, pp. 520-525, IEEE 2010.
[19]. Mengbo Hou, Qiuliang Xu, "Constructing Secure Two-Party Authenticated Key Agreement Protocol Based on Certificateless Public Key Encryption Scheme," Proceedings of 4th International Conference on Computer Science & Education, IEEE 2009.
[20]. Tarjei K. Mandt, Chik How Tan, "Certificateless Authenticated Two-Party Key Agreement Protocols," ASIAN 2006, LNCS 4435, pp. 37–44, Springer-Verlag 2007.
[21]. SHI Yijuan, LI Jianhua., "Two-Party Authenticated Key Agreement in Cerfiticateless Public Key Cryptography," Wuhan University Journal of Natural Sciences, 12 (1), pp. 071-074, 2007.
[22]. WANG Shengbao, CAO Zhenfu it, WANG Licheng, "Efficient Certificateless Authenticated Key Agreement Protocol from Pairings," Wuhan University Journal of Natural Sciences, Vol. 11 No. 5, pp. 1278-1282, 2006
[23]. Mohammad Sabzinejad Farash, Mahmoud Ahmadian Attari, "A Pairing-free ID-based Key Agreement Protocol with Different PKGs," International Journal of Network Security, Vol.16, No.2, PP.144-149, Mar. 2014.
[24]. Xuefei Cao, Weidong Kou, Xiaoni Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," Information Sciences, 180 (2010) 2895–2903, Elsevier 2010.
[25]. Robert W. Zhu, Guomin Yang, Duncan S. Wong, "An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices," Theoretical Computer Science 378 (2007) pp. 198–207, Elsevier 2007.
[26]. Seyed-Mohsen Ghoreishi, Shukor Abd Razak, Ismail Fauzi Isnin and Hassan Chizari, "New Secure Identity-Based and Certificateless Authenticated Key Agreement Protocols Without Pairings," 2014 International Symposium on Biometrics and Security Technologies (ISBAST), IEEE 2014.
[27]. Xiufeng Zhao, Qiuliang Xu, Hao Wang, "Provably Secure Identity-Based Key Agreement Protocols under Simple Assumption," International Conference on Information Theory and Information Security, IEEE, 2010.
[28]. Liang Ni, Gongliang Chen, Jianhua Li, Yanyan Hao, "Strongly secure identity-based authenticated key agreement protocols," Computers and Electrical Engineering 37 (2011) 205–217, Elsevier 2011.
[29]. Hua Guo, Zhoujun Li, Yi Mu, Xiyong Zhang, "Provably secure identity-based authenticated key agreement protocols with malicious private key generators," Information Sciences 181 (2011) 628–647, Elsevier 2011.
[30]. Takeshi Okamoto, Raylin Tso, Eiji Okamoto, "One-Way and Two-Party Authenticated ID-Based Key Agreement Protocols Using Pairing," MDAI 2005, LNAI 3558, pp. 122–133, Springer-Verlag 2005.
[31]. Marko Hölbl, Tatjana Welzer, Boštjan Brumen, "An improved two-party identity-based authenticated key agreement protocol using pairings," Journal of Computer and System Sciences 78 (2012) pp. 142–150, Elsevier 2012.
[32]. NI Liang, CHEN GongLiang, LI JianHua, HAO YanYan, "Strongly secure identity-based authenticated key agreement protocols in the escrow mode," Science China Information Sciences, 55, 2012.
[33]. Chu-Hsing Lin, Hsiu-Hsia Lin, "Secure One-round Tripartite Authenticated Key Agreement Protocol from Weil pairing," Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05), IEEE 2005.
[34]. Minghui Zheng, Huihua Zhou, Jing Chen, "An efficient protocol for two-party explicit authenticated key agreement," Concurrency and Computation: Practice and Experience (2013), Published online in Wiley Online Library (wileyonlinelibrary.com).
[35]. Ch. Asha Jyothi, G. Narsimha, J. Prathap, Gorti Vnkv Subba Rao, "Two-Party Threshold Key Agreement Protocol for Manets using Pairings," Global Journal of Computer Science and Technology: E Network, Web & Security, Volume 15 Issue 4 Version 1.0 July-1 2015.
[36]. Ch. Asha Jyothi, G. Narsimha, J. Prathap, " Two-Party Key Agreement Protocol for MANETs based on Verifiable Secret Sharing Scheme," International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 16 (2015) pp 36890-36894.
[37]. Weijun Zhang , Yonghui Han , Lulin Liu, "A Novel Key Agreement Protocol Based on Bilinear Pairing," 3rd International Conference on Biomedical Engineering and Informatics (BMEI 2010), pp. 2717-2720, IEEE 2010.
[38]. D. Freeman, M. Scott, E. Teske, "A taxonomy of pairing-friendly elliptic curves," Journal of Cryptology (2010) 23, pp. 224–280.
[39]. Hongtu Li, Liang Hu, Wei Yuan, Jianfeng Chu, Hongwei Li, "A key distribution protocol based on WDH assumption," Advanced in Control Engineeringand Information Science, Procedia Engineering 15 (2011) 1695 – 1699, Elsevier, 2011.