Identity-based Signcryption Groupkey Agreement Protocol Using Bilinear Pairing

Sivaranjani Reddi,
Anil Neerukonda Institute of Technology and Science, Bhimunipatnam, India
E-mail: sivaranjani.cse@anits.edu.in

Surekha Borra
K.S. Institute of Technology, Bangalore, India
E-mail: borrasurekha@gmail.com

Keywords: bilinear pairing, encryption, group key agreement, signcryption

Received: January 2, 2017

This paper proposes a key agreement protocol with the usage of pairing and Malon-Lee approach in key agreement phase, where users will contribute their key contribution share to other users to compute the common key from all the users key contributions and to use it in encryption and decryption phases. Initially the key agreement is proposed for two users, later it is extended to three users, and finally a generalized key agreement method, which employs the alternate of the signature method and authentication with proven security mechanism, is presented. Finally, the proposed protocol is compared with the against existing protocols with efficiency and security perspective.

Povzetek: Razvit je nov varnostni protokol za uporabo več ključev.

1 Introduction

Key Establishment is the procedure in which more than one user launches the session key, and is consequently used in accomplishing the cryptographic services like confidentiality or integrity. In general, key establishment protocols follow the key transfer approach, where one user decides the key and communicate it to other user. In contrast, for key agreement protocols all the users in the communication are involved in key establishment process. Further, these key agreement protocols provides the implicit authentication if the user assures that no other user or intruder involved in the communication knows the confidential key value. Hence, a protocol which possesses the implied key authentication to all the users involved in the group communication is called authenticated group key agreement protocol. Key Confirm is one property of the group key agreement protocol where one user involved in group communication assures that the other user in the group is under the control of the confidential key. When a protocol possesses both implicit authentication and key confirmation, that protocol is called as explicit key authentication. More details about key agreement protocols are discussed in [1, 21, 22, 23, 24].

This paper emphasis is on an authentic key agreement technique. Diffie-Hellman [2] proposed first key agreement. However, it is insecure against middle attack. Afterwards, many key agreement methodologies were published by various authors, but some users prerequisite a Public Key Infrastructure (PKI), needs more calculation and preserving efforts. Shamir[4] had initiated the concept called cryptosystem using user identity in which users public key can be calculated using the users unique attributes (e.g. Email, mobile no. etc), his private key is estimated by the trustworthy user referred as Private Key Generator (PKG). After that public key crypto system is formulated using user identity, which had simplified the process of key administration thus become a substitute to certificate centred PKI. Later, Joux[3] had proposed, Bilinear pairing based group key agreement protocol.

Boneh[5],formally published an ID based encryption scheme using bilinear pairings. Many protocols were proposed [13, 11, 10, 8, 15], analyzed and some of them were broken [14,9,17,12,16]. Few pairing based applications use a pairing-friendly elliptic curve of prime numbers. There are different coordinate systems that can be used to represent points on elliptic curves such as Jacobian, Affine and Homogeneous. Inversion to multiplication ratio threshold can be used to decide the efficiency of coordinate system. In this work timing results of pairing is being reported for both affine and projective coordinates using BN-curve. All fast algorithms to compute pairings on elliptic curves are based on *so as* Miller's algorithm [26]. In this paper, focus is on ID based authenticated key agreement using pairings with the two users. It is based on the signature scheme suggested Malone-Lee [6]. Furthermore, it is elaborated and evaluated against some of the existing ones in terms of efficiency and security. Pairing based mathematical properties were discussed in section 2, Marko Hölbl protocol the existing protocol was discussed in section 3, the proposed protocol was explained in section 4 and the next talks about performance of proposed technique against the existing protocols and finally it was concluded.

2 Preliminaries

This section presents a notation of bilinear pairing operations which are to be used next.

Bilinear maps[5] [6]: Let (G_1,+), (G_2,+) and (G_T, ・) are the two additive and one multiplicative group of prime order q > 2k for a security parameter k ϵ N, then there exists a bilinear map ê : $G_1 \times G_2 \to G_T$ that has the following properties:

1. Bilinearity: ê (aP, bQ) = ê $(P,Q)^{ab}$, where P,Q Є G_1, and a, b Є Z, can be reformulated as: e(P + Q,R) = e(P,R) e(Q,R) and e(P,Q + R) = e(P,Q)e(P,R) for P,Q,R Є G_1
2. Non-degeneracy: ê (P, Q) = 1, if Q Є G_2iff P = 1 Є G_1.
3. Computability: ê (P, Q) is efficiently computable if P Є G_1 and Q Є G_2.

When G_1=G_2 and P=Q then that group is termed as symmetric bilinear map.

2.1 Signcryption

Signcryption is a type of crypto mechanism and offers security services. It performs encryption and data signing in a single operation, and satisfies the requirements of smaller bandwidth and less computational cost by doing the operations sequentially. In symmetric encryption schemes it is computationally impossible to extract the plaintext from the signcrypted message without receiver's private key. As in symmetric digital signature, creation of signcrypted text without using the private key of the sender is computationally infeasible. Some of the existing signcryption mechanisms are as follows:

A. Malone -Lee ID-based encryption scheme[6]

The detailed description of the Malonee Lee identity based encryption is as follows:

Step 1: (Setup): A PKG considers hash functions $H_1: \{0,1\}^* \to G_1$, $H_2: \{0,1\}^* \to Z_q^*$, $H_3: G_{2\to} \{0,1\}^l$ and a generator P. The PKG can choose a random integer as master private key s and calculates P_{pub}=sP. Finally publishes the parameters <$P, \hat{e}, P_{pub}$, H_1, H_2, H_3>, by keeping PKG's secret keys as secret.

Step 2: (Extract): For given user identification $ID \in \{0,1\}^*$, the PKG calculates the public key $QID= H_1(ID)$ and secret key $SID=$ s*QID.

Step 3: (sign): For the given secret key SID and message M ∈ $\{0,1\}^*$, the sender selects random number r ∈ Z_q^*, and U=rP, then computes r=H_2(U|| M), W= r*P_{pub}, V=r*SID+W, y=e(W,QID), x=$H_3(y)$ and C=x⊕ M, finalizes the signature as (C,U,V) and then send it to receiver side.

Step 4:(unsigncrypt): Upon receiving the signature (C,U,V), receiver computes public key of the sender using his identity $QID= H_1((ID)$, parse the signature (C,U,V) then computes y=e(SID,U), x=$H_3(y)$, M=x⊕ C, r=H_2(U|| M), and then accepts M if e(V,P)= e(U,P_{pub})*e$(QID, P_{pub})^r$

Advantages: Eliminates distribution of the public key. Authentication of the public key is implicitly guaranteed as long as individual user kept his private key secure.

Disadvantage: Establishment of the secure channel is required between the user and the PKG.

B. Boneh IBE cryptosystem[5]

Boneh has proposed an identity based encryption technique to encrypt the message using pairing. It mainly contains four algorithms described as follows:

Step 1: (Setup): A PKG considers two hash functions, H_1 and H_3. The PKG can choose random s ∈ Z_q master private key, and calculates P_{pub}=sP. Finally, publishes the parameters <$P, \hat{e}, P_{pub}$, H_1, H_3>, by keeping PKG's secret keys as secret.

Step 2: (Extract): For the given user identity $(ID) \in \{0,1\}^*$ the PKG calculates publickey $QID= H_1((ID)$ and secret key $SID=$ s*QID.

Step 3: (encrypt): An user can choose r, then calculates ciphertext(C) for M, be C= (rP, M⊕$H_3(g_{ID}{}^r$)) where g_{ID}= e (QID, P_{pub})

Step 4: (decrypt): from the received C= (U, V) receiver computes V ⊕H_3(e (SID, U)) in order to extract M.

Advantage: This mechanism is secure against forgery under the chosen plaintext attack under Strong Diffie Hellman(SDH) assumption without using oracle model.

Disadvantages: All the hash functions are random hash functions. Further, as the public keys are directly computed, it leads to avoidance of certificate maintenance.

C. Hesse identity based signature[25]

A signature is computed and enclosed to M before sending onto other side. Upon receiving M along with the signature; the receiver tries to verify the signature before accepting the M. The detailed Hesse mechanism is as follows:

Step 1: (Setup): A PKG considers hash function $H_1, H: \{0,1\}^* X G_2 \to Z_q^*$. The PKG can choose s master private key and calculates P_{pub}=sP. Finally publish the parameters <$P, \hat{e}, P_{pub}$, H_1, H>, by keeping PKG's secret key s as secret.

Step 2: (Extract): For given user with identity (ID), the PKG calculates the public key $QID= H_1(ID)$ and the secret key $SID=$ s*QID.

Step 3: (Sign): for the given secret keySID and M ∈ $\{0,1\}^*$, the sender selects $P_1 \in G_1$ and k ∈ Z_q^*, and then computes r= e$(P_1, P)^k$, v=H(M,r) and u=v*$SID +$ k*P_1., finalizes the signature is (u,v).

Step 4: (Verify): for a given public key QID , the received M and the signature is (u,v). The receiver computes r= $e(u,P)$e$(QID,-P_{pub})^k$ and accept if v=H (M, r).

Advantages: It is secure against adaptive chosen message attack in the random oracle model.

Disadvantages: As PKG is generating the private keys of user, there may be a scope to decrypt or sign any message without any authorization. Hence it may not be fit to attain non repudiation

2.2 Security analysis

The protocol mechanism presented in this paper is equipped with the following listed attributes:
(i) Known key Security: For each session, the participant randomly selects h_i and r_i, results separate independent group encryption key and decryption keys for other sessions. A leakage of group decryption keys in one session will not help in derivation of other session group decryption keys.
(ii) Unknown key share: In proposed protocol, each participant U_i generates a signature ρ_i using x_i. Therefore, group participants can verify the ρ_i if it is from authorized person or not. Hence, no non group participant can be impersonated.
(iii) Key compromise impersonate: Due to generation of unforgeable signature by the participant $U_{i,,}$ the challenger cannot create the valid signature on behalf of U_i. Even if participant U_j's private key is compromised by the adversary, he cannot mimic other participant U_i with U_j's private key. Hence, key is not impersonated in the proposed protocol.

3 Marko Hölbl protocol [7]

This is an ID-based signature technique using the Hess algorithm. It is a two party ID-based authenticated key agreement protocol requiring PKG. Mainly divided into system setup, private key estimation and key agreement phase.
Phase 1 (setup): In this phase PKG decides the parameters called system parameters, which helps in the derivation of common group key agreement by all the users in the communication. A PKG formulates G_1 , G_2 and $\hat{e}$ and computes the cryptographic function H, P, a random integers as PKG's private key and P_{pub} as PKGs publickey. All elements are of order q. Finally he publishes all the parameters $<G_1, G_2, P, \hat{e}, P_{pub}, H>$, by keeping PKG's secret keys as secret.
Where mapping function $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$
Primitive Generator P: P $\in G_1$
Random integer s: s $\in Z_q^*$
Public Key P_{pub} =sP
Hash function H: $Z_q^* \rightarrow G_1$

Phase 2 (Private key extraction): In this phase PKG derives the public key Q_i and private key S_i of individual user by using their identity ID_i and then broad casts the public key and firmly send the privatekey to the respective user through secured channel, where $Q_i = H(ID_i)$ and $S_i = s*Q_i$.

Phase 3 (Key agreement): Since signature verification will authenticate the data in deciding which user issued this, a message generated from this phase will be used later to derive the session key. After choosing the receiver (B), sender (A) decides the message and then signed the message. Later on both message and the signature are sent to the receiver. The receivers compute the signature from the received message and then compare against the received signature, before deriving the key sent by sender. Procedure 1 shows the operations summary in key agreement phase.

Global Parameters $<G_1, G_2, P, \hat{e}, P_{pub}, H>$

User A Key Generation
a $\in Z_q^*$
$T_A = aP, U_A = \hat{e}(S_A, P)^a$,
$V_A = H(T_A, r_A)$, W_A = H$(V_A S_A + aS_A)$

User B Key Generation

b $\in Z_q^*$
$T_B = bP, U_B = \hat{e}(S_B, P)^b$,
$V_B = H(T_B, r_B)$,
W_B = H$(V_B S_B + bS_B)$

Calculation of secret key by User A

U_B'=$\hat{e}(W_B, P)\hat{e}(Q_B, -P_{pub})^{V_B}$
V_B=H(T_B,U_B')
K_{AB}=aT_B=abP

Calculation of secret key by User B

U_A'=$\hat{e}(W_A, P)\hat{e}(Q_A, -P_{pub})^{V_A}$
V_A=H(T_A,U_A')
K_{AB}=bT_A=abP

Procedure 1: Marko Hölbl protocol.

Marko Hölbl protocol mechanism results in the following computational requirements:

- In order to exchange message, each user has to compute two scalar multiplications, exponentiation, hash function and summation.
- In session key computation, 2 pairings and 2 hashing operation, scalar multiplication and exponentiation are required.

4 Proposed protocols

Group key agreement is the mechanism where two or more users are involved in the derivation of the group key used to encrypt/decrypt the data. The major phases in the proposed algorithm are: setup, extract, signcrypt and unsigncrypt phases as shown in Fig.1. This section describes the key agreement protocol between two users, three users and n numbers of users.

4.1 Proposed protocol for two users

This protocol is designed based on the Malone-Lee [6] ID-based crypto system scheme. It is protected against chosen random oracle model under BDH. The advantage of this algorithm is to perform the message encryption and decryption in only one step to attain security services more efficiently, instead of first signing and then encryption. This scheme is the combination of Boneh IBE cryptosystem with the variant of Hesses Identity based signature.

Step 1: (Setup): This phase usually finalizes the number of users willing to join the group communication. Once the number of users is decided, then PKG will finalize the common parameters to be used in the derivation of other phase parameters. A PKG considers three hash functions H_1, $\mathrm{H}_2, \mathrm{H}_3$ and P. PKG can choose a random integer s, master private key and calculates $\mathrm{P}_{\mathrm{pub}}$=sP. Finally publishes the parameters <P, ê, $\mathrm{P}_{\mathrm{pub}}$, $\mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3$>, by keeping PKG's secret key s as secret.

Step 2: Extract: PKG employs user's identity information in the derivation of secret and public keys. The input for this phase is user identity and produces QID and D. PKG uses user A Identity (ID_A) $\in \{0,1\}^*$and calculates public key QID_A= $\mathrm{H}_1(\mathrm{ID}_\mathrm{A})$ and secret key SID_A= s* QID_A. Once generated $\mathrm{SID}_\mathrm{A}$is securely sent to user A. This process repeats for user B, in calculating QID_B and SID_B using the identity(ID_B).

Step 3: Signcrypt: Both users A and B can execute this phase in parallel, where individual user uses their SID, along with other users public key QID and their key contribution k in the derivation of ciphertext and the signature generation.

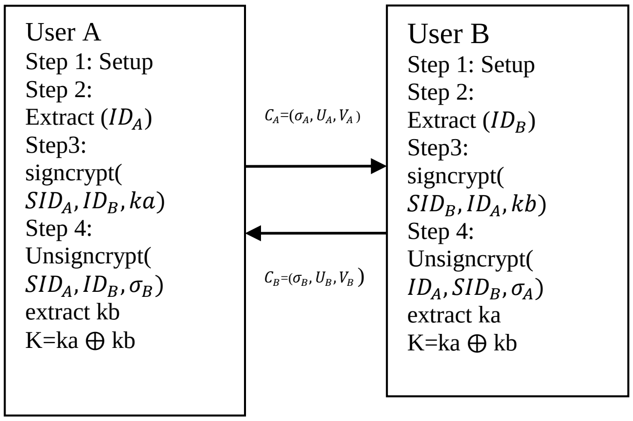

Figure 1: Group key agreement protocol.

The steps for the signcrypt at user A side is as follows:

a. User A selects ka $\in \{0,1\}^l$, computes QID_B= $H_1(ID_B)$. ------(1)
b. User A chooses a random number $X_A \leftarrow Z_q^*$ and set $U_A = X_A$P -----(2)
c. Calculates R_A= $H_1(U_A\ ||ka)$, W_A= $X_A.P_{pub}$, V_A= $R_A.SID_A + W_A$, Y_A =e(W_A, QID_B) , T_A=$H_3(Y_A)$. ---(3)
d. *Finally computes* σ_A= T_A⊕ *ka and then sends* C_A=(σ_A, U_A, V_A) *to B. ----(4)*

Here A chooses the key ka and communicates to B by adding a signature for the verification. Parallely B also chooses his contribution in key agreement kb, User B follows the above steps, uses his private key SID_B and A's public key QID_A and then sends C_B=(σ_B, U_B, V_B) to A.

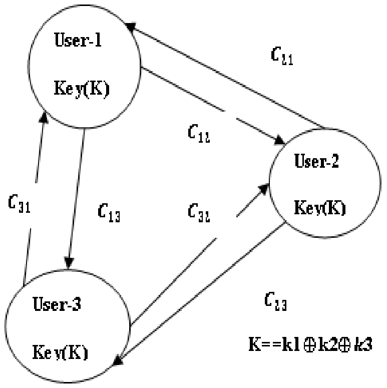

Figure 2: Key agreement among three users.

Step 4: Unsigncrypt: Key contribution of A can be extracted from C_A after comparing the signature validation condition. B uses the following steps in the derivation of ka from received C'_A.

a) Computes the A's public key QID_A=$H_1(ID_A)$ ---(5)
b) parse C'_A=(σ'_A, U'_A, V'_A), compute Y'_A =e(SID_B, U'_A) , T'_A=$H_3(Y'_A)$, ka'= T'_A⊕σ'_A and R'_A= $H_1(U'_A\ ||ka)$. ---(6)
c) Accept ka' when e(V'_A, P) = $e(QID_A, P_{pub})^{R'A}$.e(U'_A,P_{pub}) ------(7)

Limitations of the work:

- Proposed technique withstands outsider attacks (i.e. adversary is not permitted to exhibit the sender's private key with which the cipher text was created).
- Another limitation is due to the procedure used by the receiver in non repudiation. The receiver needs to prove to the third party that sender is the authorized person of a given plaintext.

4.2 Group key agreement with three users

The proposed algorithm is extended to three users and their arrangement is shown in Figure 2, where, the setup and extraction phase is same as described in section 3. During the signcrypt phase, user-1 uses other users public key with whom he wants to share the key and then computes the respective value C1, j where j ∈{3,2}. From the diagram, user-1 calculates C_{12} and C_{13} and send to user-2 and user-3 respectively. Similarly user-2 calculates their contributions C_{21} and C_{23} and then send to user 1 and 3. After signcrypt phase each user will receive the encrypted contributions from other users in the group. All the keys will be decrypted and then extract the individual key user contributions after validating the signature. Once all user signatures were satisfied, individual user adds his contribution and apply the XOR operation on all the users in group in order to derive the session group key.

4.3 Generalized group key agreement

Step 1: (Setup): This phase usually finalizes the number of users willing to join in the group communication. Once the users joining task gets completed, then PKG will finalize the common parameters to be used in the derivation of other phase parameters. A PKG considers hash functions H_1, H_2, H_3 and P. PKG can choose a random integer s, master private key and calculates P_{pub}=s*P. Finally publish the parameters <$P, \hat{e}, P_{pub}$,H_1, H_2, H_3>, by keeping PKG's secret key s as secret.

Step 2: Extract: PKG uses individual user's identity information in the derivation of secret and public keys. The input for this phase is user identity and produces QID and SID which represents public and private keys respectively. PKG uses user i (1≤ i ≤n) identity $(ID_i)$and computes QID_i= $H_1(ID_i)$ and secretkey SID_i= s*QID_i, then sends SID_isecurily to i.

For i=1 to n
Calculate QID_i= $H_1(ID_i)$ ---(8)
Calculate SID_i= s* QID_i ---(9)

Step 3: Signcrypt: Each user derives the parameters individually to other participant and communicates. User-1 in the group will first decide ka and then calculates other variables:X_1, U_1, R_1, W_1, $Y_{1,i}$,V_1 and $T_{1,i}$. Similarly user-i uses the signcrypt algorithm to securely share his key contribution ki.

a. A selects ki ∈ $\{0,1\}^l$, computes QID_j= $H_1(ID_j)$ (1≤ j ≤n, j≠ i) ---(10)

b. Afterwards he chooses a random number $X_i \leftarrow Z_q^*$ and set $U_i = X_i$P ---(11)

c. Calculates R_i= $H_1(U_i\ ||ki)$, W_i= $X_i.P_{pub}$, V_i= $R_i.SID_i + W_i$ ---(12)

d. For each user j (j≠ i) , user i computes $Y_{i,j}$ =e(W_i, QID_j) , $T_{i,j}$=$H_3(Y_i)$.---(13)

e. Finally computes $\sigma_{i,j}$= $T_{i,j}$⊕ ka and then sends $C_{i,j}$=($\sigma_{i,j}, U_A, V_A$) user –j (1≤ j ≤n, j≠ i).---(14)

Step 4: Unsigncrypt: User-j uses the following steps in the derivation of ki from received $C'_{i,j}$. key contribution of i^th user can be extracted from $C_{i,j}$ after comparing the signature validation condition

a.. Computes the i's public key QID_i=$H_1(ID_i)$ ---(15)

b.Parse $C'_{i,j}$=($\sigma'_{i,j}, U'_i, V'_i$), compute Y'_i =e(SID_j, U'_i), T'_i=$H_3(Y'_i)$, ki'= T'_i⊕σ'_i and R'_i= $H_1((U'_i\ ||ki)$. -(16)

c.Accept ki' when e(V'_i, P)=$e(QID_i, P_{pub})^{R'_i}$.e(U'_i,P_{pub}).

--- (17)

5 Performance analyses

Proposed protocol is compared with Wang [16], Yuan-Li [18], Chow–Choo without escrow[19], Choie-jeong-Lee[20] and Marko Hölbl et.al [7]. Tables 1&2 illustrate comparison of the suggested protocol against the existing protocols. The efficiency is estimated by considering the communication cost and the execution cost. Communication cost includes number of rounds and the length of message transmitted through the network during protocol execution. Overall number of rounds in protocol is the primary concern in practical environments where the group users are more in number. Yuan-Li has one round operation in key agreement phase, used one multiplication and exponentiation, one addition. Protocol is secured against the key impersonation, backward and forward secrecy. Wang's method almost uses the same number of operations as yuan's method, but computation time is more. Chow–Choo without escrow key agreement protocol mainly contains two rounds: one is extract phase and the other is key agreement phase. During the extract phase, one hash function and pairing function, remaining operations were used during the key agreement phase.

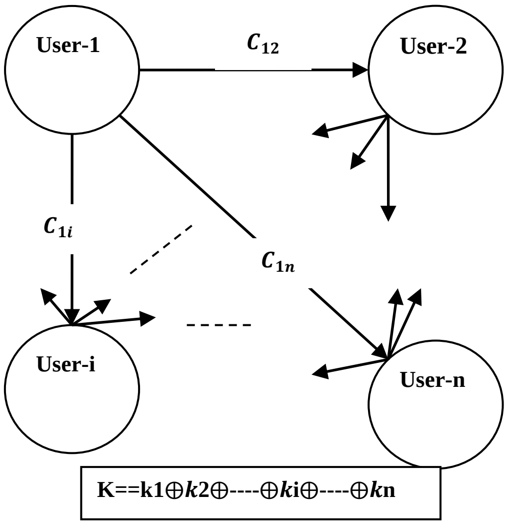

Figure 3: Generalized key agreement Protocol.

Protocol Name	Computation Cost						Commu -nication Cost
	pairing	Mul	Exp	Add	Hash	XOR	
[16]	1	3	0	3	3	0	1
[18]	1	3	0	2	1	0	1
[19]	1	4	0	2	1	0	2
[20]	2	4	0	0	2	0	1
[7]	3	3	2	1	3	0	3
Proposed	1	5	0	1	4	1	3

P2P: total point to point communication per user: Pairing: total number of mapping or pairing operations per user: Add: Total number of addition operations per user: Exp : total exponentiations performed per user.: Mul: total scalar multiplications computed : XoR: total XOR operations computed; Hash: total hash functions evaluated per user : Rounds: Number of Rounds

Table 1: Efficiency Comparison with other protocols.

Protocol name	KKS	FoS	UKS	BS	KC	KI
[16]	√	√	√	√	√	√
[18]	√	√	√	√	√	√
[19]	√	√	√	√	√	√
[20]	√	√	√	√	√	√
[7]	√	√	√	√	√	√
Proposed	√	√	√	√	√	√

KI:Key Impersonation BS:Backward Secrecy UKS:Unknown Key Share FoS:Forward Secrecy; KC:Key control

Table 2: Security Analysis with existing protocols.

Marko Hölbl et.al method uses three multiplications, three pairings, two exponentiations, one addition, and three hashing operations in three rounds for finalizing group key using pairing based key agreement. roposed algorithm has three rounds setup, private key extraction and common key agreement in the group. The computation time for proposed protocol is less compared to [7] and [20] protocols because of less number of pairing operations. The proposed protocol requires more time in scalar multiplication and XOR operation. The protocol does not require any exponential operations. Inspite of more number of hash functions, the proposed protocol requires less computation time because of involvement of less expensive operations.

6 Conclusion

An enhanced ID-based authenticated key agreement protocol is proposed and discussed, which employs signatures to authenticate participated user and verifies correctness of transferred messages between two users. The effectiveness and security of proposed technique showed all desired security properties and was compared against existing protocols in terms of efficiency and security. The protocol further confirms all the security properties with minimum time efficiency. In future, the protocol can be extended to hierarchical and cluster based network environment for establishing a secured communication. Also it can be applied in IoT based machine to machine communication, and machine to device communication.

7 References

[1] A. Menezes, P.C. Van Oorschot, S. Vanstone,(1997) Handbook of Applied Cryptography, CRC Press,.

[2] W. Diffie, M. Hellman,(1976), New directions in cryptography, IEEE Trans. Inform. Theory 22 (6),pp. 644–654.

[3] A. Joux(2000), A one round protocol for tripartite Diffie–Hellman, in: 4th International Symposium on Algorithmic Number Theory, in: Lecture Notes inComput. Sci., vol. 1838, Springer, New York, pp. 385–394.

[4] A. Shamir(1985), Identity-based cryptosystems and signature schemes, in: Advances in Cryptology – CRYPTO'84, Springer, New York, pp. 47–53.

[5] D. Boneh, M. Franklin (2003), Identity-based encryption from the Weil pairing, SIAM J. Comput. Vol,32 issue-3,pp: 586–615.

[6] J.Malonee-Lee(2002), "Identitity based signcryption, Available at *http://eprint.iacr.org/2002/098*

[7] Marko Hölbl et.al(2012)," An improved two-party identity-based authenticated key agreement protocol using pairings,journal of computer and system sciences ,vol:78,pp.142-150.

[8] L. Chen, C. Kudla(2003), Identity based authenticated key agreement protocols from pairings, in: Computer Security Foundations Workshop, IEEE, USA,pp. 219–233.

[9] K.K.R. Choo, McCullagh–Barreto(2005)," two-party ID-based authenticated key agreement protocols",Internat. J. Netw. Secur.vol-1,issue-3,pp.154–160.

[10] N. McCullagh, P.S.L.M. Barreto(2004), A new two-party identity-based authenticated key agreement, Cryptology ePrint Archive Report .

[11] K. Shim(2003), Efficient ID-based authenticated key agreement protocol based on Weil pairing, Electronics Lett. 39 (8) ,pp.653–654.

[12] K. Shim(2005), Cryptanalysis of two ID-based authenticated key agreement protocols from pairings, Cryptology ePrint Archive Report 2005/357.

[13] N.P. Smart(2002), Identity-based authenticated key agreement protocol based on Weil pairing, Electronics Lett. 38 (13) ,pp.630–632.

[14] H.M. Sun, B.T. Hsieh(2003), Security analysis of Shim's authenticated key agreement protocols from pairings, Cryptology ePrint Archive Report 2003/113.

[15] Y. Wang(2005), Efficient identity-based and authenticated key agreement protocol, Cryptology ePrint Archive Report2005/108.

[16] S.B. Wang, Z.F. Cao, H.Y. Bao(2005), Security of an efficient ID-based authenticated key agreement protocol from pairings, in: Parallel and Distributed Processingand Applications – ISPA2005, in: Lecture Notes in Comput. Sci., vol. 3759, Springer, New York, pp. 342–349.

[17] G. Xie(2004), Cryptanalysis of Noel McCullagh and Paulo S.L.M. Barreto's two-party identity-based key agreement, Cryptology ePrint Archive Report 2004/308.

[18] Q. Yuan(2005), S. Li, A new efficient ID-based authenticated key agreement protocol, Cryptology ePrint Archive Report 2005/309.

[19] Z. Cheng, L. Chen(2007), " On security proof of McCullaghBarretos key agreement protocol and its variants" , Internat. J. Secur. Networks 2 ,pp.251–259.

[20] Y.J. Choie, E. Jeong, E. Lee (2005), Efficient identity-based authenticated key agreement protocol from pairings, Appl. Math. Comput. 162 (1) ,pp.179–188.

[21] Chakraborty, S., Chatterjee, S., Dey, N., Ashour, A. S., & Hassanien, A. E. (2017). Comparative

Approach Between Singular Value Decomposition and Randomized Singular Value Decomposition-based Watermarking. In Intelligent Techniques in Signal Processing for Multimedia Security (pp. 133-149). Springer International Publishing..

[22] Dey, N., Samanta, S., Yang, X. S., Das, A., & Chaudhuri, S. S. (2013). Optimisation of scaling factors in electrocardiogram signal watermarking using cuckoo search. International Journal of Bio-Inspired Computation, 5(5), 315-326. NilanjanDey et al.(2015), "Tamper Detection of Electrocardiographic Signal using Watermarked Bio-hash Code in Wireless ", International Journal of Signal and Imaging Systems Engineering , Volume 8, Issue 1-2 .

[23] Dey, N., Pal, M., & Das, A. (2012). A Session Based Blind Watermarking Technique within the NROI of Retinal Fundus Images for Authentication Using DWT, Spread Spectrum and Harris Corner Detection. arXiv preprint arXiv:1209.0053..

[24] Hess, F. (2002, August). Efficient identity based signature schemes based on pairings. In International Workshop on Selected Areas in Cryptography (pp. 310-324). Springer Berlin Heidelberg..

[25] Beuchat, J. L., González-Díaz, J. E., Mitsunari, S., Okamoto, E., Rodríguez-Henríquez, F., & Teruya, T. (2010, December). High-speed software implementation of the optimal ate pairing over Barreto–Naehrig curves. In International Conference on Pairing-Based Cryptography (pp. 21-39). Springer Berlin Heidelberg.