EFFICIENT KEY GENERATION IN NEW MULTI-PARTY KEY AGREEMENT PROTOCOL

Vijayalakshmi P R
Professor
Computer Science and Engineering
K.L.N. College of Engineering

Abstract. Today's computing environments such as internet conferencing, distributed simulation, multi-user games, and many more applications involve Dynamic Peer Groups (DPGs). Regardless of the application environment, security services are necessary to provide communication privacy and integrity. Also, at the same time, the communication must be fast and cost-effective. In the recommended identity-based authenticated key agreement scheme, bilinear mapping is used to compute the secret key. Since the bilinear mapping computing imposes a greater computational cost, it is utilized only during the secret key computation. The proposed scheme is compared with the other related protocols by considering the computation and transmission costs. The computation costs are analyzed in terms of number of cryptographic operations. The transmission load of messages is considered as the transmission costs in the proposed identity-based scheme.

IndexTerms **- Key agreement protocol, bilinear mapping, dynamic peer groups, communication privacy, integrity, secret key**

I INTRODUCTION

Group Key Management is one of the fundamental cryptographic primitives. For the establishment of group communication, a single common group key, which is highly dynamic, is distributed to every member of the group, in heterogeneous environment. The key is refreshed whenever a member joins or leaves the group. There has been intensive research on key distribution protocols and key agreement protocols.

Many key agreement protocols are proposed (Smart 2002) which have the limitations that the group members are not mutually authenticated; dynamic group membership is not supported; or the cost of key establishment is substantial. Another common limitation of these schemes is that the group members must exchange public information to perform key establishment before they start communicating. That is, a public server is needed to keep the public information of all members for user‟s queries. In some cases, however, it is difficult to maintain a public information center and to make it always available to all users.

A research direction in key agreement protocol aims to generalize two-party key agreement sets to multi-party key agreement sets.

Authenticated Group Key Agreement-Giinther‟s (AGKA-G) protocol proposed by (Perrig 1999) suggests a contributory key agreement for secure group communication. It is based on a trusted Key Authentication Center (KAC) and Certificate Authority (CA).

As an alternative to certificate-based PKIs, Shamir (1984) introduced the concept of identity-based cryptosystems in which the users‟ identity or some other information was combined with their identity to compute one‟s public key, to achieve user authentication and key exchange. Thus, a verifier does not verify the certificates of the public keys. Meanwhile, no on-line system authority is required. The user‟s private key can be calculated by a trusted authority. However, the identity-based cryptosystems were not fully used until 2001.

An application of identity-based cryptosystems is identity-based authenticated key agreement protocols. In general such protocol includes a number of entities (the usual settings include 2, 3 or n entities) and a trusted authority referred as Key Generation Center (KGC).

The first two-party identity-based authenticated key agreement protocol which is based on the RSA algorithm was proposed by (Okamoto 1988), whereas the first two-party identity-based authenticated key agreement protocol based on the difficulty of computing a discrete logarithm problem (Elgamal 1985). Later, it was developed into International Standards, for example. PKCS #3 (1993) and ANSI X9.42 (1994).

Several identity based key agreement protocols (Chen and Kudla 2003) (McCullagh & Barreto 2005) (Sakai et al 2000) (Scott 2002) (Shim 2003) (Smart 2002) (Choo et al 2014) have been proposed since then. Most of them are not practical or do not have all required security properties. Then, feasible identity based encryption schemes based on Weil or Tate paring were introduced by (Sakai et al 2000) and later by (Boneh and Franklin 2003) independently.

Since Boneh and Franklin‟s (2001) pioneering work on the Identity-based Encryption (IBE) system, several researchers have been attempted to establish ID-based Authenticated Key Agreement Protocol (ID- AGKA). (Choi et al 2004) (Du et al 2003) proposed two ID-AGKA protocols from bilinear pairings and BD (Burmester & Desmedt 1995) schemes. However, these two protocols are vulnerable to impersonation attack. To prevent such an attack, Zhang and Chen suggest adding a time parameter to the message being signed. However, (Shim 2007) showed that the protocol is still insecure against insider colluding attacks. (Lin et al 2006) proposed a multiparty key agreement protocol, but their protocol has disadvantages in number of rounds, pairing computation and communication bandwidth. (Zhou and Zhou 2013) proposed a one-to-many mapping shared key agreement, which is based on one-to-many encryption mechanism model, but the round number of their scheme is two.

To realize group key agreement and extend Joux et al"s protocol, (Barua et al 2003) first proposed a three-group and a two-group Diffie- Hellman key agreement protocol. After that, many protocols were proposed in (Chen and Kudla 2003) (Xiehua & Yongjun 2012) (Zhang et al 2012) (Hao et al 2012) (Makri & Konstantinou 2011). (Kamal 2013) proposed an attack on Piao et al"s scheme which describes a polynomial-based key management scheme for secure intra-group and inter-group communication. (Rajaram and Dorairaj 2011) proposed an interval-based key agreement approach which adpots re-keying. To decrease the number of rounds and make AGKA more efficient, (Shi et al 2005) proposed one round ID-based AGKA protocol with bilinear parings and which can generate the secret session key in one round. Shi et al"s protocol just requires one round and less transmitted data, so it has good efficiency. However, in their protocol, if two or more than two users" long-term private keys are compromised, the adversary can compute the previous session key. So, their protocol cannot provide perfect forward secrecy. Similarly, their protocol also cannot prevent KGC from escrowing the established session keys.

Based on Weil and Tate pairing techniques, (Smart 2002) (Chen & Kudla 2003) (Scott 2002) (Shim 2003) (McCullagh & Barreto 2005) designed identity based and authenticated key agreement protocols. (Chen & Kudla 2003) showed that Smart"s protocol is not secure in several aspects. (Cheng et al 2004) pointed out that Chen-Kudla"s protocol is not secure against unknown key share attacks. (Sun and Hsieh 2003) showed that Shim"s protocol is insecure against key compromise impersonation attacks or man in the middle attacks. (Choo 2004) showed that McCullagh and Barreto"s protocol is insecure against key revealing attacks. (McCullagh and Barreto 2005) revised their protocol. But the revised protocol does not achieve weak perfect forward secrecy property. (Wang Y 2012) proposed an efficient identity-based and authenticated key agreement protocol that achieves weak perfect forward secrecy but requires some pre-computation to reduce the computational cost.

In some situations, using the certificates has undeniable restrictions, an identity-based key agreement protocol is proposed. The proposed protocol emphasizes the filtering of malicious users at the beginning of the conference to ensure that all the users obtain the same secret key. Since computing bilinear pairing imposes a greater computational cost on a protocol to improve the efficiency, bilinear pairing is used just to generate the secret key. The proposed protocol and the efficiency analysis is given in section II and III.

II PROPOSED PROTOCOL

The proposed protocol is implemented in Java. The secret key is generated each time whenever a new user joins or an already existing user leaves the communication. If no user joins or leaves, the secret key is refreshed for each 5 seconds. The generated key is verified using MARS algorithm and also the time taken for key generation is computed.

2.1 Notations Used

The notations shown in Table 1 are used to describe and analyze the protocol.

Table 1 The notations

Notation	Definition
p, q	large prime numbers
$GF(p)$	prime field of characteristic p
g	q - order generator
Z_q^*	The non-zero residues mod q
x_i	Long-term public-key of user U_i
y_i	Long-term private-key of user U_i
$e(\dots)$	The bilinear pairing
a_i	A random number selected by user U_i
k_{ij}	common session key shared with user U_j
CK_i	subkey of user U_i
T	timestamp
d_{ij} , $d_{ij}{}'$	values shared with user U_j
ID_i	identity of user U_i
SK	Secret key

2.2 Key Derivation

The proposed protocol has four phases, including parameter generation phase, secret distribution and commitment phase, subkey computation phase and secret key computation phase.

2.2.1 Parameter Generation Phase

The system authority selects the following parameters and functions and declares them publicly:

i) $\boldsymbol{p}$: a large prime number comprised $\boldsymbol{2q + 1}$, where $\boldsymbol{q}$ is also a large prime;

ii) $\boldsymbol{g}$: a $\boldsymbol{q}$-order generator over $\boldsymbol{GF(p)}$

Each user U_i is provided with the following pair of two corresponding keys:

i) Private key denoted as $\boldsymbol{x_i} \in \boldsymbol{Z_q^*}$

ii) Public key denoted as $\boldsymbol{y_i} = \boldsymbol{g^{xi} \bmod p}$

The protocol starts up the initiator who calls for a conference by initializing a set of participants $\boldsymbol{U}$. First, let $\boldsymbol{U} = \boldsymbol{U_1}, \boldsymbol{U_2}, \dots, \boldsymbol{U_n}$ be the initial participant set. Each participant $\boldsymbol{U_i}$ $\boldsymbol{1 \le i \le n}$ is a part of $\boldsymbol{U}$. In addition, the function of timestamp $\boldsymbol{T}$ is used, and it will be updated to a new one in each conference section.

2.2.2 Secret Distribution and Commitment Phase

All the participants U_i of U execute the following steps to distribute his / her subkey to other participants.

Step 1: Randomly select an integer $a_i \in Z_q^*$, calculate the common session key k_{ij} and share with all other participants U_j using the public key y_j of U_j as

$$k_{ij} = y^{a^i}{}_j \bmod p \bmod q, 1 \le j \le n \quad (1)$$

Step 2: Randomly select a line $L(X)$ as

$$L(X) = \big(c_i(\bmod q)\big)X + CK_i \quad (2)$$

where $c_i = g^{ai} \bmod p$ and CK_i is the subkey that U_i offers to share with the other participants

$$CK_i = ID_i \oplus k_{ij} \quad (3)$$

Step 3: Calculate the values d_{ij} and d'_{ij} using the session key k_{ij} and the polynomial L(X) as

$$d_{ij} = L\big(k_{ij}\big) * y_i, \ 1 \le j \le n \quad (4)$$

$$d'_{ij} = k_{ij} \oplus d_{ij}, \ 1 \le j \le n \quad (5)$$

and

$$S\,ID_i = g^{ID_i} \bmod p \quad (6)$$

Step 4: Broadcast the message

$$M_i = \{T, c_i, S\,ID_i, d'_{i1}, d'_{i2}, \dots, d'_{in}\} \quad (7)$$

2.2.3 Subkey Computation Phase

Each participant $U_i \in U$ recovers the subkey CK_i using the received message $M_j = \{T, S\,ID_j, c_j, d,'_{j1}, d'_{j2}, \dots, d'_{jn}\}$ according to the following steps:

Step 1: Check the time stamp T in advance, if it is invalid, terminate the subkey computation phase.

Step 2: Calculate the common session key k_{ji} that is shared with all other participants U_j using the individual private key x_i and the value c_j as

$$k_{ji} = c_j^{x_i} (\bmod p) (\bmod q), 1 \le j \le n \quad (8)$$

Step 3: Calculate the subkey CK_j using the session key k_{ji} and the values d_{ji} ' and c_j as

$$d_{ji} = d'_{ji} \oplus k_{ji}, \ 1 \le j \le n \quad (9)$$

$$CK_j = \left(\frac{d_{ji}}{y_j}\right) - c_j \ (\bmod q) k_{ji}, 1 \le j \le n \quad (10)$$

2.2.4 Secret key Computation Phase

When the previous phase is executed, each participant U_i in the set of $U' = \{U'_1, U'_2, \dots . U'_m\}$ calculates the secret key SK as

$$SK = e(CK_1, CK_2, \dots, CK_m) \quad (11)$$

where $\boldsymbol{e}$ is a bilinear mapping function.

III EFFICIENCY ANALYSIS

The proposed protocol is compared with Tzeng‟s protocol , Huang et. al‟s protocol and Farash et. al‟s protocol to analyze efficiency. The performance is analyzed in terms of computation costs and transmission costs. Computation costs include cost of calculating the conference key message and transmission costs include transmission load of messages broadcasted by each

participant.

Modular addition, modular subtraction and exclusive OR operations have lower computation costs in opposed to modular multiplication or modular exponential operations. Hence, those operations are ignored in calculating the computation costs to make the efficiency estimation easier. The mathematical notations assumed for calculating various operations are listed in Table 2.

Table 2 Definitions of mathematical notations

Notation	Definition
$T_L(n)$	The time for establishing an n-power Lagrange polynomial interpolation
$T_{P(n)}$	The time for calculating the output of an n-power polynomial
T_E	The time for modular exponentiation operation
T_M	The time for modular multiplicative operation
T_H	The time for executing the adopted one-way hash function H
T_I	The time for modular inverse operation
T_{PA}	The time for point addition
$\mid x \mid$	The bit length of x
n	The total number of participants

The analysis of computation costs with the related previous protocols is shown in Table 3. The Table shows that the proposed protocol does not involve any hashing function but involves less number of modular exponentiation operations compared with Huang et. al protocol. As far as Farash et. al protocol is concerned, it involves more number of scalar multiplication and each key computation involves one modular multiplication, one scalar multiplication and one point addition.

Table.3 Analysis of computation costs

Protocol	Tzeng	Huang et al	Farash et al	Proposed
Secret distribution and commitment phase	$1\,T_L\,n + n\,T_P\,n + n + 2\,T_E + 2\,T_M + 1\,T_H + 1\,T_I$	$n + 2\ T_E + n + 2\ T_M + 1\,T_H$	$4n\,T_M$	$n + 2\ T_E + n + 2\,T_M$
Protocol	**Tzeng**	**Huang et al**	**Farash et al**	**Proposed**
Subkey computation and verification phase	$n\,T_L\,n + 4n\,T_E + n\,T_M + n\,T_H$	$4n\,T_E + n\,T_M + n\,T_H$	$2\,T_M + 2\,T_{PA}$ (for each key)	$2n\,T_E + n\,T_M$
Number of session keys for 2 Rands	1	1	9	1
Key authentication	Signature based	Signature based	Certificate based	ID based

Table 4 compares transmission load where T represents the bit length of time stamp T. Although the protocol that uses the time stamp has a heavier cost in terms of the length of , they can protect against replay attack.

Table 4 Analysis of transmission costs

Tzeng	Huang et. al	Farash et. al	Proposed
$n + 1\ q$ $+ 2\ p$	$n + 1\ q$ $+ 2\ p$ $+ T$	$n + 1\ q$ $+ 2\ p + T$	$n\ q + 2\ p$ $+ T$

In addition to computation and transmission costs analysis, the secret key computation time taken for various key lengths has been analyzed in Pentium system and given in Table 5.

Table 5 Secret key computation time

Key length (bits)	Computation time (ms) (more frequent at lower bound)		
	Huang et al	Farash et al	Proposed
512	Between 137 & 640	Between 152 &760	Between 120 & 650
256	Between 52 &172	Between 49 & 230	Between 40 & 150
128	< 41 (39 ms. – frequent)	< 27 (23 ms. – frequent)	< 50 (30 ms. – frequent)

The time taken to calculate the secret key with different key sizes such as 512, 256 and 128 bits in various schemes are shown graphically in the Figure 1. It is also clear that the proposed scheme takes minimal time to generate the secret key when compared with other two schemes.

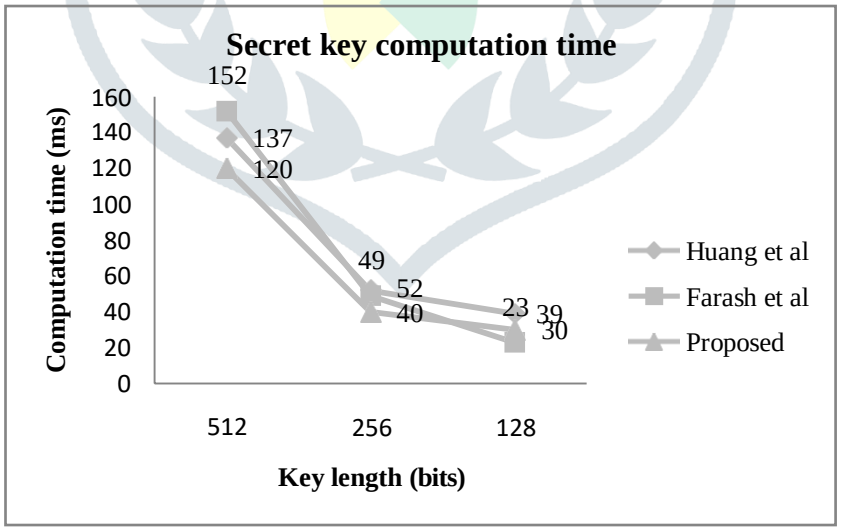

Figure 1 Secret key computation time

The efficiency of the Huang et al, Farash et al and the proposed protocol with 512 bits key length has also been analyzed and given in Table 6 and the comparative results are also shown graphically in the Figure 2.

Table 6 Proposed protocol efficiency (Key length 512 bits)

No. of participants	Total Communication Time (ms)		
	Huang et al	Farash et al	Proposed
2	1002	1236	997
3	1339	1415	1331
4	1782	1912	1569

In Farash et al scheme, 9 session keys are generated. So, the transmission time is more. The transmission time in Huang et al scheme includes the signature verification time. Figure 2 shows that the transmission time in the proposed scheme is less when compared with the other two schemes.

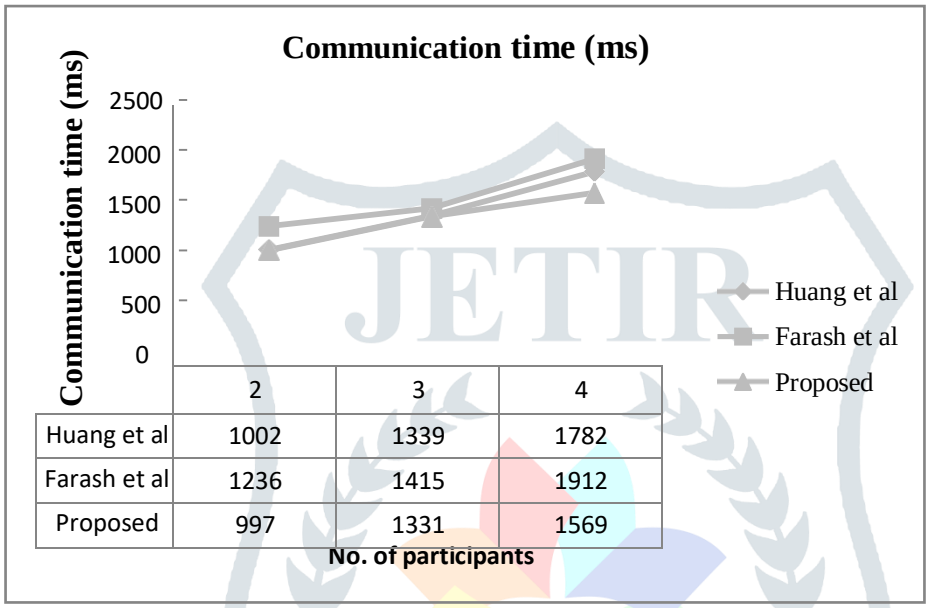

Figure 2 Communication time (Key length 512 bits)

The secret key computation time will be very negligible in the real time computing environment, because the real time responses are in the order of milliseconds and sometimes microseconds. The key can be refreshed between smaller time intervals and the improved throughput in real-time systems will not affect the performance of the system. The long-term keys of any of the participants do not compromise the session keys established in previous protocol runs. By setting very small time limit, the perfect forward secrecy can be improved.

IV CONCLUSION AND FUTURE WORK

In this paper, multi-party authenticated key agreement protocols such as identity-based authenticated key agreement protocol is proposed. Some of the existing related protocols are reviewed and the proposed protocol is compared with them. The various related protocols are compared by considering the computational complexities. It is also proved that the proposed protocol is efficient. With today‟s cloud-based environments, there are multiple data centers which spread across through multiple vendors. Data controls can be implemented using an efficient authenticated key agreement protocols.

REFERENCES

[1] American National Standards Institute 1994, “Public key Cryptography for the Financial Services Industry: Management of Symmetric Algorithm Keys Using Diffie-Hellman”, Accredited Standards Committee X9 Working Draft, Ansi X9,42.

[2] Barua, R, Dutta, R & Sarkar, P 2003, “Extending Joux‟s protocol to multi party key agreement”, Cryptography ePrint Archive, Report 62.

[3] Boneh, D & Franklin, M 2001, “Identity-based encryption from the Weil pairing”, Lecture Notes in Computer Science, Vol. 2139, pp. 213-29.

[4] Boneh, D & Frannklin, M 2003, “Identity-based encryption from the Weil pairing”, SIAM J. Computing, Vol. 32, no. 3, pp. 586-615.

[5] Burmester, M & Desmedt, Y 1995, "A secure and efficient conference key distribution system", Lecture Notes in Computer Science, Vol. 950, pp. 275-86.

[6] Chen, L & Kudla, C 2003, "Identity based authenticated key agreement protocols from pairings", In: Proceedings of the 16th IEEE computer security foundations workshop, IEEE Computer Society Press, pp. 219-33.

[7] Cheng, Z, Nistazakis, M, Comey, R & Vasiu, L 2004, "On indistinguishability-based security model of key agreement protocols-simple cases", In: Proc. of ACNS 04.

[8] Choi, K, Hwang, J & Lee, D 2004, "Efficient ID-based group key agreement with bilinear maps", Lecture Notes in Computer Science, Vol. 2947, pp. 130-44.

[9] Choo, K 2004, "Revisit of McCullagh-Barreto two party id-based authentication key agreement protocols". http://eprint.iacr.org/2004/343.pdf

[10] Choo, KR, Nam, J & Won, D 2014, "A mechanical approach to derive identity-based protocols from Diffie–Hellman-based protocols", Information Sciences, Elsevier, Vol. 281, pp. 182-200.

[11] Du, X, Wang, Y, Ge, J & Wang, Y 2003, "ID-based Authenticated Two Round Multi-Party Key Agreement", Cryptology sPrint Archive, Report 247.

[12] Elgamal, T 1985, "A public key cryptosystem and a signature protocol based on discrete logarithms", IEEE Trans. on Information Theory, Vol. 31, pp. 469-72.

[13] Hao, B, Yang, Y, Luo, S, Yang, Y & Liu, F 2012, "An Authenticated Clustering-based Group Key Agreement for Large Ad Hoc Networks", Advances in Information Sciences and Service Sciences, Vol. 4, no. 7, pp. 281-91.

[14] Kamal,AA 2013, "Cryptanalysis of a Polynomial-based Key Management Scheme for Secure Group Communication", International Journal of Network Security, Vol. 15, no. 1, pp. 68-70.

[15] Lin, CH, Lin, HH & Chang, JH 2006, "Multiple Key Agreement for Secure Teleconferencing", Systems, Man and Cybernetic (SMC), Vol. 5, pp. 3702-7.

[16] Makri, E & Konstantinou, E 2011, "Constant round group key agreement protocols: A comparative study", Computers & Security, Elsevier, Vol. 30, pp. 643-678.

[17] McCullagh, N & Barreto, PSLM 2005, "A new two-party identity- based authenticated key agreement", In: Proceedings of the CT- RSA 2005, LNCS, Vol. 3376, Springer-Verlag, pp.262-274.

[18] Okamoto, E 1988, "Key distribution systems based on identification information, Theory and Applications of Cryptographic Techniques" on Advances in Cryptology, Lecture Notes in Computer Science, Springer, USA, Vol. 293, pp. 194-202.

[19] Perrig, A 1999, "Efficient collaborative key management protocols for secure autonomous group communication", In: International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC"99), pp. 192-202.

[20] PKCS 1993, "Diffie-Hellman Key-Agreement Standard", RSA Laboratories, Redwood City, California.

[21] Rajaram, M & Dorairaj, ST 2011, "An Interval-based Contributory Key Agreement", International Journal of Network Security, Vol. 13, no. 2, pp. 92-7.

[22] Sakai, R, Ohgishi, K & Kasahara, M 2000, "Cryptosystems based on pairing", In: 2000 Symp. on Cryptography and Information Security (SCIS 2000), Okinawa, Japan.

[23] Scott, M 2002, "Authenticated ID-based key exchange and remote log-in with insecure token and PIN number", http://eprint.iacr.org/2002/164.pdf

[24] Shamir, A 1984, "Identity based cryptosystems and signature schemes", In: Proceedings of the CRYPTO"84, LNCS, Springer- Verlag, Vol. 196, pp. 47-53.

[25] Shi, Y, Chen , G & Li , J 2005, "ID-based one round authenticated group key agreement protocol with bilinear pairings", Information Technology: Coding and Computing (ITCC), Vol. 1, pp. 757-61.

[26] Shim, K 2007, "Further Analysis od ID-based Authenticated Group Key Agreement Protocol from Bilinear Maps", IEICE TRANSACTIONS, E90-A, Vol. 1, pp. 295-8.

[27] Shim, K 2003, "Efficient ID-based authenticated key agreement protocol based on the Weil pairing", Electronics Letters, Vol. 39, no. 8, pp. 653-4.

[28] Smart, NP 2002, "An identity based authenticated key agreement protocol based on the Weil pairing", Electron Lett, Vol. 38, no. 13, pp. 630-2.

[29] Sun, S & Hsieh, B 2003, "Security analysis of Shim"s authenticated key agreement protocols from pairing", http://eprint.iacr.org/2003/113.pdf

[30] Wenmin, L, Qiaoyan, W, Qi, S, Hua, Z & Zhengping, J 2012, "Password-authenticated multiple key exchange protocol for mobile applications", China Commun, Vol. 9, no. 1, pp. 64-72.

[31] Xiehua, L & Yongjun, W 2012, "Security Enhanced Authentication and Key Agreement Protocol in Next Generation Mobile Network", International Journal of Advancements in Computing Technology, Vol. 4, no. 3, pp.215-22.

[32] Zhang, L, Li, G, Xiong, C & Zhu , S 2012, "A Pairing-free Identity- based Authenticated Key Agreement Protocol for Wireless and Mobile Networks", International Journal of Advancements in Computing Technology, Vol. 4, no. 5, pp. 287-94.

[33] Zhou, J & Zhou, X 2013, "Key Agreement Protocol in DSN", TELKOMNIKA Indonesian Journal of Electrical Engineering, Vol. 11, no. 2, pp. 809-18.