A Simple and Secure Key Agreement Protocol to Integrate a Key Distribution Procedure into the DSS[1]

[1]Shu-Fen Chiou, [*2]Min-Shiang Hwang, [3]Song-Kong Chong
[1]*Department of Computer Science and Engineering, National Chung Hsing University 250 Kuo Kuang Road, Taichung, Taiwan 402, (R.O.C.), s9356055@cs.nchu.edu.tw*
[*2]*Department of Computer Science and Information Engineering, Asia University No. 500, Lioufeng Road, Wufeng Shiang, Taichung, Taiwan(R.O.C). mshwang@asia.edu.tw (Corresponding author)*
[3]*Department of Computer Science and Information Engineering, National Cheng-Kung University, No.1, University Road, Tainan City 701, Taiwan (R.O.C.)*

Abstract

A simple and secure method to integrate the Diffie-Hellman (DH) key exchange into the Digital Signature Standard (DSS) is presented in this paper. Two parties are able to establish a DH key securely between them over a public channel so our message can be encrypted. We have demonstrated how the replay attack and known key attack can be defeated. And our extended proposed protocol can be achieved with the mutual authentication requirement.

Keywords: *Cryptography, Data security, Digital signature, Digital Signature Algorithm (DSA), Digital Signature Standard (DSS), Key exchange*

1. Introduction

In a public communication channel, it is difficult to require any two parties to keep a pre-established secret key before a communication is set up. It means an uncountable size of key table is needed to maintain secretly. The key distribution scheme proposed by Diffie and Hellman (DH) was the first public key algorithm to solve this problem [5][19]. The DH key exchange can be used for the key distribution, where two parties can use the algorithm to establish a secret key over insecure channels by using a public communication only [3][8][9][12][14]. However, it cannot be used to encrypt and decrypt messages. The DH key exchange is vulnerable to a man-in-the-middle attack so that the communicating parties cannot ensure who is on the other side actually when running the DH key exchange algorithm [4][20-21][30-31]. Therefore, a signature to the exchanged key is needed [1-2][7][10-11][15-18][24-29][32-33].

In 1993, Arazi suggested that the integration of the DH key exchange with the Digital Signature Algorithm (DSA), which introduced by Digital Signature Standard (DSS) [13][22] could provide a compact key distribution scheme [1]. The scheme gives “free of charge” to the DH key exchange when the modular exponentiation operations are executed when both the DSA and the DH key exchange are integrated. Later, Nyberg and Rueppel pointed out the exchanged shared secret keys (DH keys) were not mutually independent; if one of the secret key was compromised, then the others would be revealed as well [23]. In 2004, Harn et al. extended Arazi’s approach and proposed three different protocols to integrate the DH key exchange with the DSA for an authenticated exchanged key securely [6]. However, Harn et al. need an assumption in their protocols, which implies that the public key of a receiver should be known by a sender before running the protocols.

It should be noted that, by using Arazi’s scheme, without the knowledge of the public key of the opposite side, a party is able to establish a DH key with the other side directly over a public channel. The party simply replaces the *message* in the DSA with a DH key exchange element, e.g. g^v mod p, and sends it to the other party with the corresponding *signature* and *certificate*.

[1] Partial results have been published in ICNIT 2012

The receiver can check the signature by using the information recorded in the certificate. Then, the receiver performs the similar operations as the sender. Consequently, a shared secret key K can be established.

However, by using Harn et al.'s protocol, a party needs to know the public key of the receiver before they can establish a shared secret key securely. Although the requirement that the parties should know each other's public key is not considered to be a big disadvantage, we consider this additional requirement has already violated Arazi's original conception of the work, which means that a party who lacks the public key of the opposite side at the moment can also establish a shared secret key securely by using the DH + DSA algorithm. We deem that this is the essence of the DH key exchange, as well as Arazi's original conception of the work.

On the other hand, we consider the previous protocols [1][6] are vulnerable to replay attack. An attacker simply intercepts the old messages m_A, s_A sent by user A, and then replays them to the user B afterward; user B is unable to determine if it is a replay or not, and vice versa. We shall demonstrate how this attack can be defeated without increasing the computation burden of the parties.

In this paper, a simple method is proposed to secure the scheme proposed by Arazi. We will present how the known key attack shown by Nyberg and Rueppel as well as the replay attack can be prevented, and our extended proposed protocol can achieve the mutual authentication.

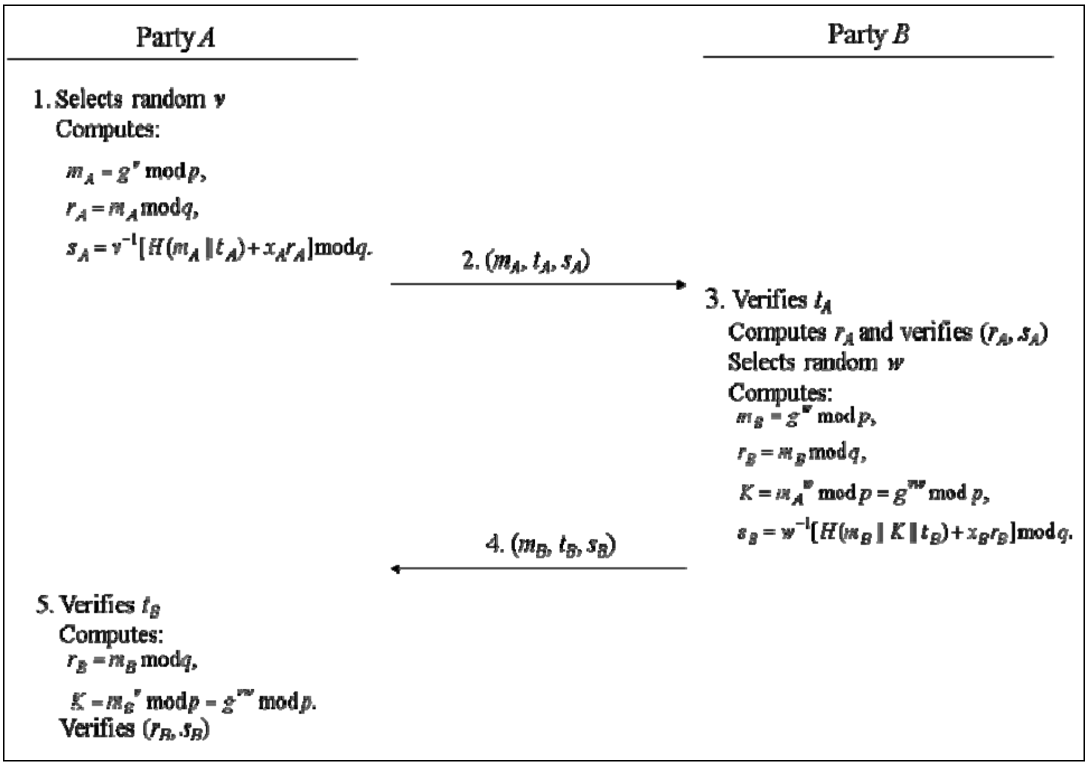

Figure 1. The flowchart of proposed method

2. The Proposed Protocol

In this section, we will introduce our proposed protocol. In our proposed protocol, suppose that there are two parties, A and B, and they will establish a shared secret key K by the public channel. Then we will introduce the extended protocol if we can know the public key of the receiver before the transmission. The extended protocol can not only establish a share secret key K, but also achieve the mutual authentication requirement.

2.1. Notations

We first give some notations used in our proposed protocol. In DSA, p is a large prime number with L bits in length, $2^{L-1} < p < 2^L$, $512 \le L \le 1024$, and L is a multiple of 64; q is another large prime, where $2^{159} < q < 2^{160}$ and $q|(p\text{-}1)$; g is an integer of multiplicative order q in Zp; $g = h^{(p-1)}=q \bmod p$, where $1 < h < p\text{-}1$; $x(0 < x < q)$ is a user's private key; $y = g^x \bmod p$ represents the corresponding public key; $\{p, q, g, y\}$ are public values; $H(.)$ is a one-way hash function, yielding a 160-bit output.

2.2. The proposed method

In our proposed protocol, there are three steps to establish the secret key K between Party A and Party B. Figure 1 is the flowchart of the proposed protocol, and the proposed protocol is described as follows.

i. Party A randomly selects a secret value $v \in Z_q$, $0 < v < q$, and A computes m_A, r_A, and s_A as follows:

$$m_A = g^v \bmod p,$$
$$r_A = m_A \bmod q, \tag{1}$$
$$s_A = v^{-1}[H(m_A \| t_A) + x_A r_A] \bmod q.$$

Next, A sends (m_A, t_A, s_A) to B, where t_A is a timestamp of A.

ii. Upon receiving (m_A, t_A, s_A), party B verifies t_A. If t_A is fresh, B computes $r_A = m_A \bmod q$ and verifies A's DSA signature (r_A, s_A) on message m_A and t_A. If the condition is observed, B selects a secret value $w \in Z_q$, $0 < w < q$. B computes m_B, r_B, the shared secret key K, and s_B as follows:

$$m_B = g^w \bmod p,$$
$$r_B = m_B \bmod q, \tag{2}$$
$$K = m_A{}^w \bmod p = g^{vw} \bmod p,$$
$$s_B = w^{-1}[H(m_B \| K \| t_B) + x_B r_B] \bmod q. \tag{3}$$

Next, B sends (m_B, t_B, s_B), where t_B is a timestamp of B.

iii. After party A receiving (m_B, t_B, s_B), A first verifies whether t_B is fresh or not. If t_B is fresh, A computes $r_B = m_B \bmod q$, $K = m^v{}_B \bmod p$, and verifies B's signature (r_B, s_B) on $H(m_B||K||t_B)$. If the verification holds, it means the shared secret key $K = (g^v)^w \bmod p = (g^w)^v \bmod p$ between A and B is established.

2.3. The extended protocol

In Harn et al.'s protocol, a party needs to know the public key of the receiver before they can establish a shared secret key securely. If we can know the public key of the receiver, we can achieve the external mutual authentication requirement by the extended protocol. Figure 2 is the flowchart of the extended protocol, and we describe our extended protocol by the following steps:

i. Similarly, first Party A randomly selects a secret value $v \in Z_q$, $0 < v < q$, and A computes m_A, r_A, and s_A by Equation (1). After computing, A sends (m_A, t_A, s_A) and $Sig_A(m_A, t_A, s_A)$ to B, where t_A is a timestamp of A and $Sig_A(m_A, t_A, s_A)$ is the signature signed by A with the private key of A.

ii. Upon receiving (m_A, t_A, s_A) and $Sig_A(m_A, t_A, s_A)$, party B verifies t_A. If t_A is fresh, B authenticates A by signature using the public key of A. If it is true, B computes $r_A = m_A \bmod q$ and verifies A's DSA signature (r_A, s_A) on message m_A and t_A. If the condition is observed, B selects a secret value $w \in Z_q$, $0 < w < q$. B computes m_B, r_B, the shared secret key K, and s_B by Equations (2) and (3). Next, B sends (m_B, t_B, s_B) and $Sig_B(m_B, t_B, s_B)$ to A, where t_B is a timestamp of B *and* $Sig_B(m_B, t_B, s_B)$ is the signature signed by B with the private key of B.

iii. After party A receiving (m_B, t_B, s_B) and $Sig_B(m_B, t_B, s_B)$, A first verifies whether t_B is fresh or not. If t_B is fresh, A authenticates B by signature using the public key of B. If it is true, A computes $r_B = m_B \bmod q$, $K = m^v{}_B \bmod p$, and verifies B's signature (r_B, s_B) on $H(m_B||K||t_B)$. If the verification holds, it means the shared secret key $K = (g^v)^w \bmod p = (g^w)^v \bmod p$ between A and B is established.

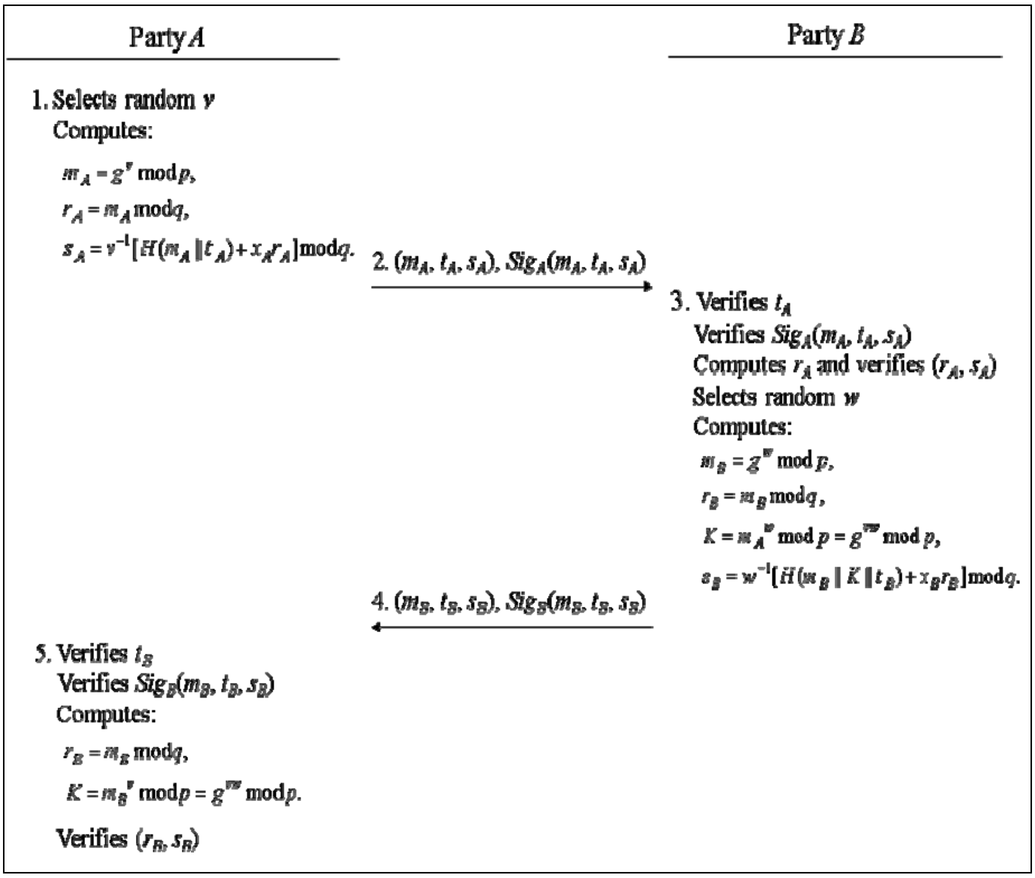

Figure 2. The flowchart of the extended method

3. Security analysis

In this section, we will analyze that our proposed protocol can defeat the replay and Nyberg and Ruppel's known key attacks, and our extended method can achieve the mutual authentication requirement.

- **Reply attack:**
  Two timestamp t_A and t_B are appended to the key exchange protocol in parties A and B, respectively. We strengthen the original protocol proposed by Arazi as well as Harn et al.'s by making the replay attack being defeated. It is easy to notice that unless the receivers store every m_A or m_B respectively, the replay attack cannot be avoided in the previous protocols. We introduce the idea of timestamp to the proposed scheme in order to avoid this weakness. Because the calculation of a one-way hash function $H(.)$ is very fast and its output length is fixed, therefore, the generation of a signature s_A or s_B is still as very efficient as the previous protocols [1][6].

- **Known key attack:**

  In the following, we shall demonstrate how the proposed protocol can withstand Nyberg and Rueppel's known key attack [23]. In the proposed protocol, each shared secret key K between A and B can be expressed by publicly known or transmitted parameters, and the quantity of $g^{x_A x_B} \bmod p$. The values of v, w, and vw can be expressed by Equations (1) and (3):

$$\begin{aligned} v &= s_A^{-1}[H(m_A \| t_A) + x_A r_A] \bmod q, \\ w &= s_B^{-1}[H(m_B \| K \| t_B) + x_B r_B] \bmod q, \\ vw &= s_A^{-1} s_B^{-1}[H(m_A \| t_A) H(m_B \| K \| t_B) \\ &\quad + H(m_A \| t_A) x_B r_B + H(m_B \| K \| t_B) x_A r_A \\ &\quad + x_A x_B r_A r_B] \bmod q. \end{aligned} \tag{4}$$

  From Equations (2) and (4), we obtain $K^{s_A s_B}$ as follows:

$$K^{s_A s_B} = g^{H(m_A \| t_A) H(m_B \| K \| t_B)} y_B^{H(m_A \| t_A) r_B} y_A^{H(m_B \| K \| t_B) r_A} (g^{x_A x_B})^{r_A r_B} \bmod p.$$

  It is easy to see that, except K and $g^{x_A x_B}$, all the other parameters are publicly known or sent between A and B. Therefore, if an attacker can obtain one of the shared secret key K between A and B, he/she can retrieve $g^{x_A x_B}$ deservedly. Assuming that the value of K is compromised in the i connection, an attacker can compute $g^{x_A x_B}$ easily. However, by using the obtained knowledge of $g^{x_A x_B}$, the attacker *is unable* to compute the shared secret key K after the i connections as well as before the i connections. The key is that party B binds the exchanged DH key K with the m_B to form $H(m_B \| K \| t_B)$ in s_B in Step (ii). Therefore the knowledge of $g^{x_A x_B}$ is useless for breaking the exchanged DH key K *of others*. Accordingly, the known key attack can be prevented. If one of the DH key K is compromised, then the others will still remain secret.

- **Mutual authentication:**

  In our extended protocol, the authentication response from party A is $Sig_A(m_A, t_A, s_A)$ signed by the private key x_A. B can verify the signature by the public key of A to authenticate A, and confirm the message is generated by A. Thus, B can generate the secret key K. A also can authenticate B after the authentication response $Sig_B(m_B, t_B, s_B)$ from party B. A can verify the signature $Sig_B(m_B, t_B, s_B)$ by the pubic key of B. Thus, our extended protocol can achieve the mutual authentication.

4. Discussion and Conclusion

We have shown how the replay attack and the flaw discussed in [23] can be avoided in this paper. The paper remains the primitive conception of the work proposed by Arazi. The parties A and B are able to establish a DH key K securely between them over a public channel, even though they do not know the public key of the opposite party beforehand. Because the calculation of a one-way hash function $H(.)$ is very fast and its output length is fixed, therefore, the generation of signatures is still as very efficient as the previous protocols [1][6]. In our extended method, if we can know the pubic key of the receiver before the transmission, we can use the condition to achieve the mutual authentication requirement.

5. Acknowledgement

The authors wish to thank many referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC 98-2221-E-468-024-MY3.

6. References

[1] B. Arazi, "Integrating A Key Distribution Procedure into the Digital Signature Standard," IEE Electronics Letters, vol. 29, no. 11, pp. 966–967, 1993.
[2] Ting-Yi Chang, Min-Shiang Hwang, and Wei-Pang Yang, "A Communication-efficient Three-Party Password Authenticated Key Exchange Protocol," Information Sciences, vol. 181, pp. 217–226, 2011.
[3] Ting-Yi Chang, Wei-Pang Yang, and Min-Shiang Hwang, "Simple Authenticated Key Agreement and Protected Password Change Protocol," Computers & Mathematics with Applications, vol. 49, pp. 703–714, 2005.
[4] Kou-Min Cheng, Ting-Yi Chang, and Jung-Wen Lo, "Cryptanalysis of Security Enhancement for A modified Authenticated Key Agreement Protocol," International Journal of Network Security, vol. 11, no. 1, pp. 55–57, 2010.
[5] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. IT-22, pp. 644–654, Nov. 1976.
[6] L. Harn, M. Mehta, and W. J. Hsin, "Integrating Diffie-Hellman Key Exchange into the Digitial Signature Algorithm (DSA)," IEEE Communications Letters, vol. 8, no. 3, pp. 198–200, 2004.
[7] Min-Shiang Hwang and Chii-Hwa Lee, "Authenticated Key-Exchange in a Mobile Radio Network", European Transactions on Telecommunications, Vo1. 8, No.3, pp.265-269, May 1997.
[8] Min-Shiang Hwang, Chih-Wei Lin, and Cheng-Chi Lee, "Improved Yen-Joye's Authenticated Multiple-Key Agreement Protocol," Electronics Letters, vol. 38, no. 23, pp. 1429–1431, 2002.
[9] Min-Shiang Hwang, Li-Hua Li, and Cheng-Chi Lee, "A Key Authentication Scheme with Non-Repudiation," ACM Operating Systems Review, vol. 38, no. 3, pp. 75–78, 2004.
[10] Min-Shiang Hwang, Jung-Wen Lo, Chia-Hsin Liu, "Enhanced of Key Agreement Protocols Resistant to a Denial-of-Service Attack," Fundamenta Informaticae, vol. 61, no. 3, pp. 389-398, July 2004.
[11] Min-Shiang Hwang, Song-Kong Chong, Hsia-Hung Ou, "On the Security of an Enhanced UMTS Authentication and Key Agreement Protocol," European Transactions on Telecommunications, vol. 22, no. 3, pp. 99-112, Apr. 2011.
[12] Wen-Shenq Juang and Jing-Lin Wu, "Efficient User Authentication and Key Agreement with User Privacy Protection," International Journal of Network Security, vol. 7, no. 1, pp. 120–129, 2008.
[13] Raj S. Katti and Rajesh G. Kavasseri, "Nonce Generation for the Digital Signature Standard," International Journal of Network Security, vol. 11, no. 1, pp. 23-32, 2010.
[14] Cheng-Chi Lee, Min-Shiang Hwang, and Li-Hua Li, "A New Key Authentication Scheme based on Discrete Logarithms," Applied Mathematics and Computation, vol. 139, no. 2, pp. 343–349, 2003.
[15] Cheng-Chi Lee, Tzu-Chun Lin, Min-Shiang Hwang, "A Key Agreement Scheme for Satellite Communications," Information Technology and Control, vol. 39, no. 1, pp. 43-47, Mar. 2010.
[16] Chun-Ta Li, Min-Shiang Hwang, Yen-Ping Chu, "Improving the Security of a Secure Anonymous Routing Protocol with Authenticated Key Exchange for Ad Hoc Networks", International Journal of Computer Systems Science and Engineering, vol. 23, no. 3, pp. 227-234, May 2008.
[17] Chun-Ta Li, Min-Shiang Hwang, Yen-Ping Chu, "A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks", Computer Communications, vol. 31, no. 12, pp. 2803-2814, July 2008.
[18] Chun-Ta Li, Min-Shiang Hwang and Yen-Ping Chu, "An Efficient Sensor-to-Sensor Authenticated Path-Key Establishment Scheme for Secure Communications in Wireless Sensor Networks," International Journal of Innovative Computing, Information and Control, vol. 5, no. 8, pp. 2107-2124, Aug. 2009.
[19] Jie Liu and Jianhua Li, "A better Improvement on the Integrated Diffie-Hellman-DSA Key Agreement Protocol," International Journal of Network Security, vol. 11, no. 2, pp. 114–117, 2010.
[20] Jung-Wen Lo, Ji-Zhe Lee, Min-Shiang Hwang, and Yen-Ping Chu, "An advanced Password Authenticated Key Exchange Protocol for imbalanced Wireless Networks," Journal of Internet Technology, vol. 11, no. 7, pp. 997–1004, 2010.
[21] Jung-Wen Lo, Shu-Chen Lin, and Min-Shiang Hwang, "A Parallel Password-authenticated Key

Exchange Protocol for Wireless Environments," Information Technology and Control, vol. 39, no. 2, pp. 146–151, 2010.

[22] National Institute of Standards and Technology (NIST), Digital signature standard (DSS), Tech. Rep. FIPS PUB 186-2, NISS, US Department Commerce, 2000.

[23] K. Nyberg and R. A. Rueppel, "Weakness in some Recent Key Agreement Protocol," IEE Electronics Letters, vol. 30, no. 1, pp. 26–27, 1994.

[24] Hsia-Hung Ou, Min-Shiang Hwang and Jinn-Ke Jan, "A Cocktail Protocol with the Authentication and Key Agreement on the UMTS," Journal of Systems and Software, vol. 83, no. 2, pp. 316-325, Feb. 2010.

[25] Yongxuan Sang, Lili Zhang, Lin You, and Zhongwen Li, "Two Non-interactive Key Agreement Protocols under Certificateless Scenarios", IJACT: International Journal of Advancements in Computing Technology, vol. 4, no. 6, pp. 331-337, 2012.

[26] Wang Tao, and Chen Wen Qing, "Three-Party Strong Password Authenticated Key Exchange Protocols," IJACT: International Journal of Advancements in Computing Technology, Vol. 3, No. 11, pp. 39-46, 2011.

[27] Wang Wei, "Session Key Agreement Protocol based on Special Threshold," IJACT: International Journal of Advancements in Computing Technology, vol. 4, no. 12, pp. 275 - 282, 2012

[28] Shuhua Wu and Yuefei Zhu, "Proof of Forward Security for Password based Authenticated Key Exchange," International Journal of Network Security, vol. 7, no. 3, 2008.

[29] Chou-Chen Yang, Ting-Yi Chang, and Min-Shiang Hwang, "Cryptanalysis of simple Authenticated Key Agreement Protocols," IEICE Transactions on Foundations, vol. E87-A, no. 8, pp. 2174–2176, 2004.

[30] Chou-Chen Yang, Jian-Wei Li, Min-Shiang Hwang, "A New Mutual Authentication and Key Exchange Protocol with Balanced Computational Power for Wireless Settings," European Transactions on Telecommunications, vol. 15, no. 2, pp. 91-99, 2004.

[31] Fuw-Yi Yang, and Zhen-Wei Liu, "An Anonymous User Identification and Key Distribution Technical Protocol," IJACT: International Journal of Advancements in Computing Technology, vol. 3, no. 8, pp. 38-49, 2011

[32] Zeng Yong, Ma Jianfeng, and SangJae Moon, "An Improvement on a Three-party Password-based Key Exchange Protocol Using Weil Pairing," International Journal of Network Security, vol. 11, no. 1, pp. 188-193, 2010.

[33] Liping Zhang, Guiling Li, Cong Xiong, and Shao-Hui Zhu, "A Pairing-free Identity-based Authenticated Key Agreement Protocol for Wireless and Mobile Networks," IJACT: International Journal of Advancements in Computing Technology, vol. 4, no. 5, pp. 287- 294, 2012.