An Efficient MQV Key Agreement Scheme

Li-Chin Hwang[1] and Min-Shiang Hwang[2]
(Corresponding author: Min-Shiang Hwang)
Department of Computer Science and Engineering, Asia University[2]
No. 500, Lioufeng Road, Wufeng Shiang, Taichung, Taiwan, R.O.C. (Email: mshwang@asia.edu.tw)
Department of Computer Science and Engineering, National Chung Hsing University[1]
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
Department of Health Services Administration, China Medical University[1]
No.91, Hsueh-Shih Road, Taichung 40402, Taiwan, R.O.C.
(Received Feb. 12, 2011; revised and accepted May 8 & Dec. 9, 2012)

Abstract

Menezes et al. proposed the first key agreement protocol (MQV) that employs a signature to sign Diffie-Hellman public keys without using a one-way hash function. The IEEE Standard Committee adopted the MQV protocol as a standard. In order to establish multiple common secret keys between two parties, Harn and Lin proposed a new protocol based on the MQV protocol. However, this protocol has a limit that only n^2-1 keys out of n^2 keys for can be used avoiding the known key attack. Afterwards, Tseng proposed a protocol that can use n keys to avoid the known key attack. In this article, we shall extend Tseng's protocol and make it able to generate $(n^2 + 1)$ keys in one session, and all the keys can be used against the known-key attack.

Keywords: Cryptography, key agreement, key authentication

1 Introduction

In 1976, Diffie and Hellman [9] proposed a public-key distribution scheme for distributing a common session key between two parties. Unfortunately, the Diffie-Hellman protocol is vulnerable to the man-in-the-middle attack, since no authentication is supported between the two parties. Many solutions [5, 7, 16, 17, 20, 24, 26, 27, 31, 33, 36] have been proposed to solve this problem. In 1995, Menezes et al. [28] proposed a famous protocol for the two parties to authenticate each other without any hash function, and the protocol was adopted as IEEE P1363-2000 standard [18]. There are many authenticated key agreement have been proposed [1, 2, 3, 4, 6, 8, 12, 14, 15, 19, 21, 22, 23, 25, 30, 34].

In order to establish multiple common secret keys between two parties efficiently, in 1998 Harn and Lin [10] designed an authenticated key agreement protocol based on the MQV protocol without using any one-way hash function. The Harn-Lin protocol enables the two parties to authenticate each other and establish n^2 common session keys. To avoid the known key attack [29], the Harn-Lin protocol sets up the limit that only $(n^2 - 1)$ common session keys can be used. Then, Yen and Joye [37] proposed a forgery attack and broke the Harn-Lin protocol, and they also proposed an improved protocol. However, according to Wu et al. [35], the Yen-Joye protocol cannot withstand the same attack that bothers the Harn-Lin protocol. Later, we proposed an improved protocol [24] to enhance the Yen-Joye protocol. Harn and Lin [11] then modified the signature signing equation in [10] to avoid the forgery attack in 2001, but their protocol still holds on to the limit that only (n^2-1) common session keys can be used. In 2002, Tseng [32] proposed a robust protocol that makes use of all the n^2 common session keys against the known-key attack.In 2013, Huang et al. proposed an efficient scheme to generate n^2+n secret keys in one session [13]. Their scheme is based on the difficulty of calculating discrete logarithms problem.

In this article, we shall improve the Tseng protocol to generate (n^2+1) common session-keys in one session, and all the keys can be used against the known-key attack.

2 Extended Tseng's Protocol

In this section, we shall propose an extended version of Tseng's protocol that can establish $(n^2 + 1)$ common session keys between two parties. The protocol is composed of two phases: the initiation phase and the multiple-key agreement phase. For simplicity, Let's suppose Bob and Alice want to establish five common session keys by using 2 short-term keys. They have to go through the following processes.

The initiation phase: As the Diffie-Hellman scheme, the system publishes a large prime number p. Bob and Alice choose their random numbers x_A and

x_B and compute the corresponding long-term public keys $y_A = g^{x_A} \bmod p$ and $y_B = g^{x_B} \bmod p$, respectively.

The multiple-key agreement phase:

1) Alice chooses two random short-term secret keys k_{A_1} and k_{A_2}, where $k_A = k_{A_1} + k_{A_2} \bmod q$. Then Alice computes the corresponding short-term public keys $r_A = g^{k_A} \bmod p$, $r_{A_1} = (y_B)^{k_{A_1}} \bmod p$ and $r_{A_2} = (y_B)^{k_{A_2}} \bmod p$. Furthermore, Alice gets the signature S_A based on the equation $s_A r_A = x_A - r_{A_1} k_A \bmod q$. Later, Alice sends $\{r_{A_1}, r_{A_2}, s_A, Cert(y_A)\}$ to Bob, where $Cert(y_A)$ is a certificate for the public key signed by a trusted party.
2) Just as Alice, Bob also generates $k_{B_1}, k_{B_2}, r_{B_1}, r_{B_2}$ and s_B and sends $\{r_{B_1}, r_{B_2}, s_B, Cert(y_B)\}$ to Alice.
3) Alice verifies the authenticated messages $\{r_{B_1}, r_{B_2}, s_B, Cert(y_B)\}$ from Bob. Alice then checks the following equation:

$$y_B = (r_B)^{r_{B_1}} g^{s_B r_B} \bmod p, \tag{1}$$

where $r_B = r_{b1} r_{b2} \bmod p$, $r_{b_1} = (r_{B_1})^{x_A^{-1}} \bmod p$ and $r_{b_2} = (r_{B_2})^{x_A^{-1}} \bmod p$. If the equation is correct, Alice generates five common session keys as follows:

$$\begin{aligned} K_1 &= r_{b1}^{k_{A1}} \bmod p, \\ K_2 &= r_{b1}^{k_{A2}} \bmod p, \\ K_3 &= r_{b2}^{k_{A1}} \bmod p, \\ K_4 &= r_{b2}^{k_{A2}} \bmod p, \end{aligned}$$

and

$$\begin{aligned} K_5 &= g^{(k_A + k_B)} \bmod p \\ &= g^{k_A} \cdot g^{k_B} \bmod p \\ &= g^{k_A} \cdot r_B \bmod p. \end{aligned}$$

Like Alice, Bob also verifies the authenticated messages and generates five common secret keys: $K_1 = r_{a1}^{k_{B1}} \bmod p$, $K_2 = r_{a2}^{k_{B1}} \bmod p$, $K_3 = r_{a1}^{k_{B1}} \bmod p$, $K_4 = r_{a2}^{k_{B2}} \bmod p$, and $K_5 = g^{k_B} \cdot r_A \bmod p$.

3 Security Analysis

The security of our extended protocol is analyzed as follows.

1) **Known-key attack:** In [32], Tseng proved that his protocol could resist the known-key attack. For the same reason, our extended protocol can also withstand the known-key attack [29]. In our extended protocol, we derive $g^{x_A \cdot x_B}$ as

$$\begin{aligned} g^{x_A x_B} &= g^{(s_A r_A + r_{A_1} k_A)(s_B r_B + r_{B_1} k_B)} \bmod p \\ &= g^{s_A s_B r_A r_B} \cdot g^{s_A r_A r_{B_1} k_B} \cdot g^{s_B r_B r_{A_1}} \\ &\quad \cdot g^{k_A k_B r_{A_1} r_{B_1}} \bmod p \\ &= g^{s_A s_B r_A r_B} \cdot g^{s_A r_A r_{B_1} k_B} \cdot g^{s_B r_B r_{A_1}} \\ &\quad \cdot (g^{(k_{A_1} + k_{A_2})(k_{B_1} + k_{B_2})})^{r_{A_1} r_{B_1}} \bmod p \\ &= g^{s_A s_B r_A r_B} \cdot g^{s_A r_A r_{B_1} k_B} \cdot g^{s_B r_B r_{A_1}} \\ &\quad \cdot (K_1 K_2 K_3 K_4)^{r_{A_1} r_{B_1}} \bmod p. \end{aligned}$$

Suppose that all the common session keys $(K_1, K_2, K_3, K_4, K_5)$ are leaked to an intruder. Even so, the intruder is still very difficult for to calculate $g^{x_A x_B}$ by intercepting the transmitted message between the two parties, where the transmitted message involves $(r_{A_1}, r_{A_2}, r_{B_1}, r_{B_2}, s_A, s_B)$. The intruder cannot derive r_A and r_B from any transmitted message. The security comes from the difficulty of calculating discrete logarithms. Therefore, the extended protocol can also withstand the known-key attack.

2) **Replay attack:** To resist the replay attack, our protocol uses short-term keys. The lifetime of the short-term keys (k_{A_i} and k_{B_i}, $i \in 1, 2, \ldots$) is only one session long, with a view to establishing $n^2 + 1$ keys. For the next session, the two parties have to randomly choose new short-term keys again. When the intruder replays the previously intercepted message to Bob for masquerading as Alice, the request will be rejected because Bob will discover the message has been used previously.
3) **Forgery attack:** Assume that an intruder wants to impersonate Alice to establish the common session keys with Bob. The intruder forges the previously intercepted message $(r_{A_1}, r_{A_2}, s_A, Cert(y_A))$ to $(r'_{A_1}, r'_{A_2}, s'_A, Cert(y_A))$ and sends it to Bob, where $(r'_{A_1}, r'_{A_2}, s'_A)$.

$$\begin{aligned} k'_A &= k'_{A_1} + k'_{A_2} \bmod q \\ r_{A_1} &= g^{k'_{A_1}} \bmod p, \\ r_{A_2} &= g^{k'_{A_2}} \bmod p, \\ s'_A r'_A &= x'_A - r'_{A_1} k'_{A_1} \bmod q. \end{aligned}$$

Bob will rejects the transmitted message from the intruder because the message cannot pass verification Equation (1).

4 Conclusions

In this paper, we have proposed an extended version of Tseng's protocol that is more efficient than [32]. Tseng's protocol can establish n^2 common session keys between two parties at one session. However, in our extended protocol, $n^2 + 1$ keys can be established, and attack is no longer a threat.

Acknowledgments

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC 101-2221-E-468-019, NSC 101-2622-E-468-002-CC3, and NSC 101-2622-H-468-001-CC3. The authors are grateful to the anonymous reviewers for valuable comments.

References

[1] 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.

[2] 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.

[3] Atul Chaturvedi and Sunder Lal, "An authenticated key agreement protocol using conjugacy problem in braid groups," *International Journal of Network Security*, vol. 6, no. 2, pp. 181–184, 2008.

[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] Shu-Fen Chiou, Min-Shiang Hwang, and Song-Kong Chong, "A simple and secure key agreement protocol to integrate a key distribution procedure into the dss," *International Journal of Advancements in Computing Technology*, vol. 4, no. 19, pp. 529–535, 2012.

[6] Kim-Kwang Raymond Choo, "Revisit of mccullagh-barreto two-party id-based authenticated key agreement protocols," *International Journal of Network Security*, vol. 1, no. 3, pp. 154–160, 2005.

[7] Kim-Kwang Raymond Choo, "On the security of lee, kim, kim, & oh key agreement protocol," *International Journal of Network Security*, vol. 3, no. 1, pp. 85–94, 2006.

[8] Kim-Kwang Raymond Choo, "Revisiting lee, kim, & yoo authenticated key agreement protocol," *International Journal of Network Security*, vol. 2, no. 1, pp. 64–68, 2006.

[9] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[10] Lein Harn and Hung-Yu Lin, "An authenticated key agreement protocol without using one-way functions," in *Proceedings of the 8th National Conference on Information Security*, pp. 155–160, Kaohsiung, Taiwan, May 1998.

[11] Lein Harn and Hung-Yu Lin, "Authenticated key agreement without using one-way hash functions," *Electronics Letters*, vol. 37, no. 10, pp. 629–630, 2001.

[12] Li-Chin Huang and Min-Shiang Hwang, "Two-party authenticated multiple-key agreement based on elliptic curve discrete logarithm problem," *International Journal of Smart Home*, vol. 7, no. 1, pp. 9–18, 2013.

[13] Li-Chin Hwang, Cheng-Chi Lee, and Min-Shiang Hwang, "A $n^2 + n$ MQV key agreement protocol," *International Arab Journal of Information Technology*, vol. 10, no. 2, pp. 137–142, 2013.

[14] Min-Shiang Hwang and Chii-Hwa Lee, "Authenticated key-exchange in a mobile radio network," *European Transactions on Telecommunications*, vol. 8, no. 3, pp. 265–269, 1997.

[15] 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.

[16] Min-Shiang Hwang, Chih-Wei Lin, and Cheng-Chi Lee, "Improved yen-joye's authenticated multiple-key agreement protocol," *IEE Electronics Letters*, vol. 38, no. 23, pp. 1429–1431, 2002.

[17] Min-Shiang Hwang, Jung-Wen Lo, and Chia-Hsin Liu, "Enhanced of key agreement protocols resistant to a denial-of-service attack," *Fundamenta Informaticae*, vol. 61, no. 3, pp. 389–398, 2004.

[18] IEEE, "IEEE Standard 1363-2000: Standard specifications for public key cryptography," *IEEE*, 1999.

[19] 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.

[20] Iuon-Chang Lin, Chin-Chen Chang, and Min-Shiang Hwang, "Security enhancement for the simple authentication key agreement algorithm," in *The Twenty-Fourth Annual International Computer Software and Applications Conference(COMPSAC)'2000*, pp. 113–115, 2000.

[21] Jeng-Ping Lin and Jih-Ming Fu, "Authenticated key agreement scheme with privacy-protection in the three-party setting," *International Journal of Network Security*, vol. 15, no. 3, pp. 179–189, 2013.

[22] 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.

[23] 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.

[24] Eric Jui-Lin Lu and Min-Shiang Hwang, "An improvement of a simple authenticated key agreement algorithm," *Pakistan Journal of Applied Sciences*, vol. 2, no. 1, pp. 64–65, 2002.

[25] Eric Jui-Lin Lu and Min-Shiang Hwang, "An improvement of a simple authenticated key agreement algorithm," *Pakistan Journal of Applied Sciences*, vol. 2, no. 1, pp. 64–65, 2002.

[26] Eric Jui-Lin Lu, Cheng-Chi Lee, and Min-Shiang Hwang, "Cryptanalysis of some authenticated key agreement protocols," *International Journal of Computational and Numerical Analysis and Applications*, vol. 3, no. 2, pp. 151–157, 2003.

[27] Rongxing Lu and Zhenfu Cao, "Off-line password guessing attack on an efficient key agreement protocol for secure authentication," *International Journal of Network Security*, vol. 3, no. 1, pp. 35–38, 2006.

[28] A. J. Menezes, M. Qu, and S. A. Vanstone, "Some key agreement protocols providing implicit authentication," in *Proceedings of 2nd Workshop Selected Areas in Cryptography*, pp. 22–32, May 1995.

[29] K. Nyberg and R. A. Rueppel, "Weakness in some recent key agreement protocol," *IEE Electronics Letters*, vol. 30, no. 1, pp. 26–27, 1994.

[30] Hsia-Hung Ou, Iuon-Chang Lin, Min-Shiang Hwang, and Jinn-Ke Jan, "TK-AKA: using temporary key on authentication and key agreement protocol on UMTS," *International Journal of Network Management*, vol. 19, no. 4, pp. 291–303, 2009.

[31] Marimuthu Rajaram and Thilagavathy Dorairaj Suresh, "An interval-based contributory key agreement," *International Journal of Network Security*, vol. 13, no. 2, pp. 92–97, 2011.

[32] Y. M. Tseng, "Robust generalized MQV key agreement protocol without using one-way hash function," *Computer Standards & Interfaces*, vol. 24, no. 3, pp. 241–246, 2002.

[33] Liming Wang and Chuan-Kun Wu, "Efficient key agreement for large and dynamic multicast groups," *International Journal of Network Security*, vol. 3, no. 1, pp. 8–17, 2006.

[34] Shengbao Wang, Zhenfu Cao, and Feng Cao, "Efficient identity-based authenticated key agreement protocol with pkg forward secrecy," *International Journal of Network Security*, vol. 7, no. 2, pp. 181–186, 2008.

[35] Tzong-Sun Wu, Wei-Hua He, and Chien-Lung Hsu, "Security of authenticated multiple-key," *Electronics Letters*, vol. 35, no. 5, pp. 391–392, 1999.

[36] 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.

[37] Sung-Ming Yen and M. Joye, "Improved authenticated multiple-key agreement protocol," *Electronics Letters*, vol. 34, no. 18, pp. 1738–1739, 1998.

Li-Chin Hwang received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 2001 and in 2003. She is currently working toward the PhD degree in the Department of Computer Science and Engineering at the National Chung Hsing University (NCTU), Taiwan. Her current research interests include information security, cryptography, medical image, and mobile communications.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. He was a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999- 2002. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. He obtained 1997, 1998, 1999, 2000, and 2001 Outstanding Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published 170+ articles on the above research fields in international journals.