An Efficient Authenticated Key Agreement Scheme Without Using Smart Card

Chun-Ta Li
Department of Information Management
Tainan University of Technology
529 Jhongjhen Road, Yongkang, Tainan, Taiwan 710, R.O.C.

Min-Shiang Hwang
Department of Computer Science & Information Engineering
Asia University
500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

Pin-Chieh Huang
Department of Electrophysics[§]
National Chiao Tung University
1001 University Road, Hsinchu, Taiwan 300, R.O.C.

Abstract

Authenticated key agreement based on passwords over insecure networks is the conventional method of secure communications in the various networking environments. In this article, we propose an efficient authenticated key agreement scheme without using smart card and the security of our proposed scheme is based on exclusive OR operation, hashing function, and discrete logarithm problem. Therefore, the proposed scheme does not need the use of any additional public-key infrastructure and it is not only secure against security attacks but also is more efficient than the other schemes.

Keyword: *Authenticated Key Agreement, Cryptography, Modification Attack, Network Security.*

1. Introduction

In 1976, Diffie and Hellman [1] first proposed a well-known key agreement scheme that the two communication parties can agree a common session key in an insecure network [2, 12, 13, 15, 16]. However, the Diffie-Hellman scheme suffers from the man-in-the-middle attack [4, 8, 18, 19]. In 1999, Seo and Sweeney [22] proposed an authenticated key agreement scheme (SAKA) in which two communication parties used a pre-shared password to achieve user authentication, but Tseng [23] demonstrated that it could not withstand the replay attack in which a malicious user could cheat an honest party into believing a wrong common session key. So then, Tseng proposed an improved scheme to against the replay attack.

Later, Ku and Wang [7] indicated that the Tseng scheme suffers from the backward replay attack without modification and modification attack [11, 14, 17]. Then, Ku and Wang proposed an improved scheme to dispose of these two attacks. In 2003, Hsu et al. [3] pointed out that the Ku-Wang scheme is vulnerable to the modification attack and also proposed an improved scheme that not only enhances the security of the Ku-Wang scheme but also is more efficient than the previous schemes. However, in 2004, Lee and Lee [10] showed that the Hsu et al. scheme is still insecure to the modification attack and further proposed an improved scheme. Lee-Lee's scheme repaired the weakness of Hsu et al. scheme and it is as efficient as the Hsu et al. scheme. Unfortunately, in 2005, Kim et al. [6] showed that the Lee-Lee scheme was breakable by guessing attack. Moreover, Lee et al. [9] also presented that the Lee-Lee scheme was breakable by man-in-the-middle attack. In this article, we proposed an improved key agreement scheme without using smart card and the improved scheme is not only suggested to eliminate the weaknesses

Table 1. Notations used in this article

Alice, Bob	Two communication parties
id_A, id_B	Identities of Alice and Bob
P	A large prime number
PW	A common password shared between Alice and Bob
Q	An integer pre-computed from PW
Q^{-1}	The inverse of $Q \pmod P$
g	A base generator $\in Z_P^*$ with the order $P-1$
a	A random number chosen by Alice
b	A random number chosen by Bob
K	A common session key derive from Alice and Bob
$H(\cdot)$	One-way hash function

in Lee-Lee scheme but also is more efficient than previously proposed schemes [5, 9, 21, 20] in terms of computation and communication loads.

The article is organized as follows. First, we propose a simple improved scheme in Section 2. In Section 3, we analyzed the security of our improved scheme and compared it with other related schemes. Finally, we conclude this article in Section 4.

2. The Proposed Scheme

In this section, we will propose a simpler key agreement scheme based on the Lee-Lee scheme [10]. The notations in Table 1 are used in this article.

The detailed steps of the proposed scheme are described as follows and in Figure 1.

Step 1: Alice computes $X_1 = g^a \oplus Q \bmod P$ and sends X_1 to Bob.

Step 2: After receiving the message X_1, Bob computes $Y_1 = g^b \oplus Q \bmod P$.

Step 3: Next, Bob computes the session key as follows:

$$X = X_1 \oplus Q \bmod P = g^a \bmod P$$
$$K_2 = X^b \bmod P = g^{ab} \bmod P.$$

Step 4: Lastly, Bob checks whether $K_2 \neq 1$ holds or not. If it holds, Bob computes $Y_2 = H(id_b, X_1, K_2)$ and sends Y_1 and Y_2 to Alice. Otherwise, the key agreement scheme is terminated.

Step 5: After receiving the messages, Y_1 and Y_2, Alice first computes the session key as follows:

$$Y = Y_1 \oplus Q \bmod P = g^b \bmod P.$$
$$K_1 = Y^a \bmod P = g^{ab} \bmod P.$$

Step 6: Then, Alice verifies $Y_2 \stackrel{?}{=} H(id_b, X_1, K_1)$ and checks whether $K_1 \neq 1$ holds or not. If above holds, Alice computes $X_2 = H(id_a, Y_1, K_1)$ and sends X_2 to Bob. If it does not hold, it means that Alice and Bob can not agree a common session key and the key agreement scheme is terminated.

Step 7: After receiving the message X_2, Bob verifies $X_2 \stackrel{?}{=} H(id_a, Y_1, K_2)$. If it holds, Alice and Bob are now confirmed that the common session key $K = K_1 = K_2 = g^{ab} \bmod P$. Otherwise, the key agreement scheme is terminated as previous circumstance shows.

3. Analysis

In this section, we analyze the security of the proposed scheme and compare the related works with ours in terms of computation and communication loads as follows.

3.1 Security Analysis

1. In our scheme, it is difficult for an attacker to derive the pre-computed integer Q from receives messages X_1, Y_1, Y_2 and X_2 because the complexity of computing Q from receives messages is a discrete logarithm problem. Therefore, our scheme is secure to against guessing attack.

2. An attacker may try to alter the messages to cheat both of communication parties into believing a wrong session key(modification attack). It does not work unless he/she knows the common session key K.

3. If an attack Eve tries to masquerade Alice and cheat Bob(masquerade attack), Eve can send the deceitful message $X_1' = g^{a'} \oplus Q'$ to Bob, where a' is randomly selected and Q' is derived from a guessed password P'. Then, Eve wants to verify whether her guess holds or not, she must check $K_2 = (g^{a'} \oplus Q' \oplus Q)^a \bmod P)$. However, Eve only has $(g^{a'} \oplus Q')$ and without knowing a. As a result, it is difficult for Eve to masquerade Alice and cheat Bob because she has to solve the discrete logarithm problem.

3.2 Performance Analysis

In this section, we compare the efficiency of the proposed scheme, the Lu-Cao scheme [20], the Ryu et al. scheme [21], the Lee et al. scheme [9], and the Hwang et al. scheme [5]. Previous schemes are briefly reviewed below.

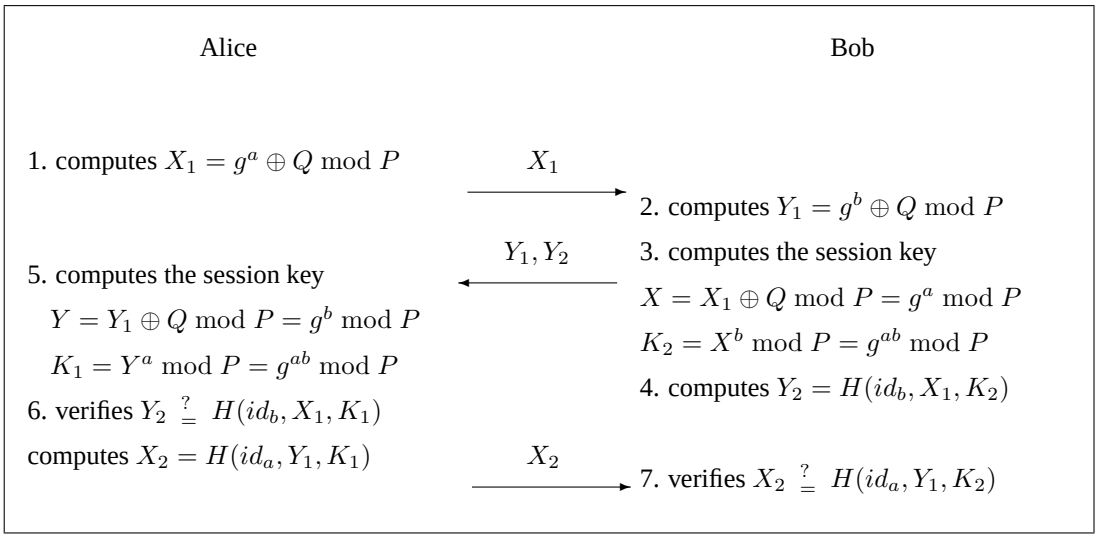

Figure 1. The proposed scheme

- The Hwang et al. Scheme [5]: There are two steps in the Hwang et al. scheme. First, the two communication parties, Alice and Bob already generated their long-term secret key X_a, X_b and generated two short-term secret keys $\{R_{a1}, R_{a2}\}$ and $\{R_{b1}, R_{b2}\}$, respectively. After two steps messages transmitted, the two communication parties, Alice and Bob are now confirmed as the four common session keys by the following equations:

$$\begin{aligned} K_{1a} &= K_{1b} = g^{Ra1Rb1} \bmod P, \\ K_{2a} &= K_{2b} = g^{Rb1Ra2} \bmod P, \\ K_{3a} &= K_{3b} = g^{Ra1Rb2} \bmod P, \\ K_{4a} &= K_{4b} = g^{Ra2Rb2} \bmod P. \end{aligned}$$

- The Ryu et al. Scheme [21]: Before the scheme begins, Alice and Bob pre-shared a password Q and knew the system parameters, including a large prime P and its generator g. First, Alice first chooses a random number a, and computes $X = g^a + Q \bmod P$ and then sends X to Bob. After receiving the message X, Bob chooses a random number b, and computes $Y = g^b \bmod P$, $Y_1 = (X - Q)^b \bmod P$, and $Y_2 = H(ID_a, X, Y_2)$. Then Bob sends Y and Y_2 to Alice. After receiving the message Y, Y_2, Alice computes $X_1 = Y^a \bmod P$ and checks if $H(ID_a, X, X_1)$ equals to Y_2 or not. If it holds, Alice computes $X_2 = H(ID_b, Y, X_1)$ and the common session key $K_1 = kdf(ID_a, ID_b, X_1)$ and sends X_2 to Bob, where $kdf(.)$ is a key derivation function. Similarly, Bob could verify the validity of X_2. If X_2 equlas to $H(ID_b, Y, Y_2)$, Bob computes the common session key $K = K_1 = K_2 = kdf(ID_a, ID_b, Y_1)$.

- The Lee et al. Scheme [9]: There are two phases in the Lee-Lee scheme, *Key establishment phase* and *Key validation phase*, respectively. Before the scheme begins, Alice and Bob publish g^X and g^Y, respectively(where $X = aQ$ and $Y = bQ$). In *Key establishment phase*, Alice first chooses a random number a, and computes $X = aQ$, $X_1 = g^X \bmod P$ and then sends X_1 to Bob. After receiving the message X_1, Bob chooses a random number b, and computes $Y = bQ$, $Y_1 = g^Y modP$ and then sends Y_1 to Alice. After receiving the message Y_1, Alice computes the common session key $K_1 = Y_1^{Q^{-1}a}$. Similarly, Bob could compute the common session key $K_2 = X_1^{Q^{-1}b}$. After that, the two communication parties, Alice and Bob could derive the common session key $K = K_1 = K_2 = g^{ab} \bmod P$. In *Key validation phase*, in order to convince the validity of the derived session key, Alice and Bob should reciprocally carry out the follow-

ing steps. First, Alice checks whether $K_1 \neq 1$ holds or not. If it holds, Alice computes $X_2 = H(id_A, X_1, K_1)$ and sends X_2 to Bob. Then, Bob verifies the validation of the equation $X_2 \stackrel{?}{=} H(id_A, X_1, K_2)$. If it holds, Bob checks whether $K_2 \neq 1$ holds or not. If it holds, Bob computes $Y_2 = H(id_B, Y_1, K_2)$ and sends Y_2 to Alice. Finally, Alice could verify the validation of the equation $Y_2 \stackrel{?}{=} H(id_B, Y_1, K_1)$. If it holds, the two communication parties, Alice and Bob are now confirmed that the common session key $K = K_1 = K_2 = g^{ab} \bmod P$.

- The Lu-Cao Scheme [20]: There are three communication steps in Lu-Cao scheme. In first step, Alice chooses a random number a, and computes $X_1 = g^{aQ} \bmod P$ and $X_2 = g_1^a \bmod P$, then sends messages X_1, X_2 to Bob. On receiving X_1 and X_2, Bob first computes $X_1' = X_1^{Q^{-1}} = g^a \bmod P$, and then chooses two random numbers b_1 and b_2 to computes $Y_1 = g^{b_1} g_1^{b_2} \bmod P$ and $Y_2 = X_1'^{b_1} X_2^{b_2} \bmod P$. In second step, Bob sends Y_1 and $Y_3 = H(A||B||X_1||X_2||Y_1||Y_2||0)$ to Alice. After receiving Bob's message, Alice first computes $Y_2' = Y_1^a \bmod P$ and then verifies $Y_3 \stackrel{?}{=} H(A||B||X_1||X_2||Y_1||Y_2'||0)$. If it holds, Alice authenticates Bob. Otherwise, the protocol is terminated. In third step, Alice sends $X_3 = H(A||B||X_1||X_2||Y_1||Y_2'||1)$ to Bob and computes the common session key $K_1 = H(A||B||X_1||X_2||Y_1||Y_2')$. On receiving X_3, Bob verifies $X_3 \stackrel{?}{=} H(A||B||X_1||X_2||Y_1||Y_2||1)$. If it does hold, Bob authenticates Alice. Finally, Bob computes the common session key $K_2 = H(A||B||X_1||X_2||Y_1||Y_2)$.

Next, we compare the efficiency of our scheme and previous related schemes in Table 2. As Table 2 shows, in terms of the computation loads, our proposed scheme is more efficient than other schemes that only four exponential operations are required and the computation loads of Hwang et al. scheme is the highest because eighteen exponential operations are required.

Furthermore, from the perspective of communication load shows, the Hwang et al. scheme is eight messages sent, two communication steps and four random numbers; The Lu-Cao scheme is five messages sent, three communication steps and three random numbers; The communication cost of the Lee et al. scheme is six messages sent(two publish messages are included), four communication steps and two random numbers; The communication cost of our scheme is four messages sent, three communication steps and two random numbers. Similarly, in terms of communication loads, our proposed scheme is more efficient than the other related schemes mentioned above.

4. Conclusion

In this article, we have proposed an efficient authenticated key agreement scheme. We also give a comparison with our scheme and some related schemes in terms of communication and computation loads. From the performance result shows, the communication and computation loads of the proposed scheme are the lowest and it is as secure as the other related schemes mentioned above.

5. Acknowledgments

We wish to thank many anonymous referees for their suggestions to improve this paper. This work was supported in part by National Science Council under the grants NSC 98-2221-E-005 -050 -MY3.

References

[1] Whitfield Diffie and M. Hellman. New directions in cryptology. *IEEE Transations on Information Theory*, IT-22(6):644–654, 1976.

[2] Marko Holbl and TITLE = Tatjana Welzer.

[3] Chien-Lung Hsu, Tzong-Sun Wu, Tzong-Chen Wu, and Chris Mitchell. Improvement of modified authenticated key agreement protocol. *Applied Mathematics and Computation*, 142(2-3):305–308, 2003.

[4] Min-Shiang Hwang, Chih-Wei Lin, and Cheng-Chi Lee. Improved yen-joye's authenticated multiple-key agreement protocol. *IEE Electronics Letters*, 38(23):1429–1431, 2002.

[5] Ren-Junn Hwang, Sheng-Hua Shiau, and Chih-Hua Lai. An enhanced authentication key exchange protocol. In *Proceedings of the 17th International Conference on Advanced Information Networking and Applications (AINA'03), IEEE*, pages 202–205, 2003.

[6] Kee-Won Kim, Eun-Kyung Ryu, and Kee-Young Yoo. Cryptanalysis of lee-lee authenticated key agreement scheme. *Applied Mathematics and Computation*, 163(1):193–198, 2005.

[7] Wei-Chi Ku and Sheng-De Wang. Cryptanalysis of modified authenticated key agreement protocol. *IEE Electronics Letters*, 36(21):1770–1771, 2000.

[8] Cheng-Chi Lee, Min-Shiang Hwang, and Li-Hua Li. A new key authentication scheme based on discrete logarithms. *Applied Mathematics and Computation*, 139(2):343–349, 2003.

Table 2. Performance comparison

	C1	C2	C3	C4	C5	C6	C7	C8	C9
Hwang et al. [5]	8	2	4	2	18	4	0	4	4
Ryu et al. [21]	4	3	2	0	4	0	6	0	1
Lee et al. [9]	6	4	2	0	6	2	4	0	1
Lu-Cao [20]	5	3	3	0	8	1	6	0	1
The proposed scheme	4	3	2	0	4	0	4	4	1

Notes. C1: needs to send messages; C2: communication steps; C3: number of random numbers; C4: number of addition operation; C5: number of exponential operation; C6: number of multiplication operation; C7: number of $H(\cdot)$ operation; C8: number of XOR operation; C9: number of common session key.

[9] Keon-Jik Lee and Byeong-Jik Lee. Cryptanalysis of the modified authenticated key agreement scheme. *Applied Mathematics and Computation*, 170(1):280–284, 2005.

[10] N. Y. Lee and M. F. Lee. Further improvement on the modified authenticated key agreement scheme. *Applied Mathematics and Computation*, 157(3):729–733, 2004.

[11] Chun-Ta Li and Yen-Ping Chu. Cryptanalysis of threshold password authentication against guessing attacks in ad hoc networks. *International Journal of Network Security*, 8(2):166–168, 2009.

[12] Chun-Ta Li and Min-Shiang Hwang. An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*, 33(1):1–5, 2010.

[13] Chun-Ta Li and Min-Shiang Hwang. An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards. *International Journal of Innovative Computing, Information and Control*, accepted, 2009.

[14] Chun-Ta Li, Min-Shiang Hwang, and 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*, 23(3):227–234, 2008.

[15] Chun-Ta Li, Min-Shiang Hwang, and Yen-Ping Chu. A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Computer Communications*, 31(12):2803–2814, 2008.

[16] 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*, 5(8):2107–2124, 2009.

[17] Chun-Ta Li, C. H. Wei, and Y. H. Chin. A secure event update protocol for peer-to-peer massively multiplayer online games against masquerade attacks. *International Journal of Innovative Computing, Information and Control*, accepted, 2009.

[18] Eric Jui-Lin Lu and Min-Shiang Hwang. An improvement of a simple authenticated key agreement algorithm. *Pakistan Journal of Applied Sciences*, 2(1):64–65, 2002.

[19] 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*, 3(2):151–157, 2003.

[20] Rongxing Lu and Zhenfu Cao. Off-line password guessing attack on an efficient key agreement protocol for secure authentication. *International Journal of Network Security*, 3(1):35–38, 2006.

[21] E. K. Ryu, K. W. Kim, and K. Y. Yoo. An authenticated key agreement protocol resistant to a dictionary attack. In *Proceedings of ICCSA 2004*, volume LNCS 3043, pages 603–610, 2004.

[22] D. Seo and P. Sweeney. Simple authenticated key agreement algorithm. *IEE Electronics Letters*, 35(13):1073–1074, 1999.

[23] Yuh-Min Tseng. Weakness in simple authenticated key agreement protocol. *IEE Electronics Letters*, 36(1):48–49, 2000.