Improving Security of A Communication-efficient Three-party Password Authentication Key Exchange Protocol

Cheng-Chi Lee[1,3], Shih-Ting Chiu[1], and Chun-Ta Li[2]
(Corresponding author: Chun-Ta Li)

Department of Library and Information Science, Fu Jen Catholic University[1]
510 Jhongjheng Rd., Sinjhuang Dist., New Taipei City 24205, Taiwan, R.O.C.
Department of Information Management, Tainan University of Technology[2]
529 Zhongzheng Road, Tainan 71002, Taiwan, R.O.C.
Department of Photonics & Communication Engineering, Asia University[3]
No. 500, Lioufeng Road, Wufeng Shiang,Taichung 402, Taiwan, R.O.C.
(Email: th0040@mail.tut.edu.tw)

(Received Mar. 29, 2013; revised and accepted Nov. 06, 2013)

Abstract

Three-party Password-based Authentication Key Exchange (3PAKE) allows a trusted server to assist two users to establish a common session key. Recently, Wu et al. pointed out that Chang et al.'s 3PAKE was vulnerable to the off-line guessing attack and proposed an improved 3PAKE to fix the problem. However, we found that Wu et al.'s protocol is still subject to the off-line guessing attack. In addition, the paper offers a simple method to detect the attack.

Keywords: Authentication, cryptanalysis, guessing attack, key exchange, password-based, three-party

1 Introduction

To verify remote users' identities, password authentication schemes are most commonly used when it comes to allowing users to choose their own passwords [5, 6, 11, 12, 22, 25, 28-30, 33-37, 43]. Lamport [16] was the first to propose a password authentication scheme, and since then password authentication schemes have prospered and developed into many new forms [1, 3, 4, 7-10, 13-15, 26, 27, 31, 32, 39, 42], among which Password-based Authentication Key Exchange (PAKE) is now a main stream.

1.1 Related Work

The first password-based authentication key exchange protocol was proposed by Bellovin and Merritt [1]. Using their PAKE protocol, two users can share a password to establish their common session key. However, PAKE cannot live up to the requirement of modern multi-user systems, so many researchers [2, 23, 24, 38, 40, 41] have endeavored to develop PAKE into three-party password-based authentication key exchange (3PAKE) protocols. In a 3PAKE design, there is a trusted server that assists two users to cooperate in establishing a common session key which they can use to communicate with each other privately [17-21].

Among the many 3PAKE protocols, Chang et al.'s work [2], which is based on LHL-3PAKE [24], is quite an outstanding design. Chang et al.'s protocol needs no server's public key and no symmetric cryptosystems, and they claim that the protocol meets such security requirements as mutual authentication, session key security, know-key security, forward secrecy, and protection against the off-line password guessing attack. Unfortunately, Wu et al. [38] pointed out the fact that Chang et al.'s protocol has a flaw against the off-line guessing attack. Wu et al. then proposed an improved protocol to remedy the security weakness.

1.2 Contributions

However, we found that Wu et al.'s protocol is still vulnerable to the off-line guessing attack. Therefore, in this paper, we will prove that even Wu et al.'s protocol is not secure enough against the off-line guessing attack. In addition, the paper offers a simple method to detect the attack.

1.3 Organization

The organization of this paper is as follows. Section 2 will be a brief review of Wu et al.'s protocol. Then, in Section 3, we will show why Wu et al.'s protocol is still vulnerable to the off-line password guessing attack. In Section 4, we will propose a simple method to detect the attack. Finally, the conclusion will be presented in Section 5.

2 Review of Wu et al.'s Protocol

In this Section, we review the three-party password

Table 1: The notations

Notations	Description
ε	An elliptic curve defined over a finite field $GF(p)$
P	A base point in ε with large order q, where q is a secure large prime
G	A cyclic additive group generated by P
$x \cdot P$	The point multiplication defined as $x \cdot P = P + P + \cdots + P$($x$ times)
Z_q	The ring of integers modulo q, $Z_q = \{0,1,\dots,q-1\}$
Z_q^*	The multiplicative group of non-zero integers modulo q
$\mathcal{H}(.)$	A one-way hash function:$\{0,1\}^* \to \{0,1\}^l$
$\Vert$	A concatenation of bit strings
A, B	Two communication clients (users) (also representing their identities)
S	The trusted server(also representing its identities)
PW_A, PW_B	A's and B's password secretly shared with S

authenticated key exchange protocol proposed by Wu et al. [38]. In Table 1 below, there are some notations used in Wu et al.'s protocol.

The structure of their protocol is illustrated in Figure 1, and the detailed steps are as follows. To begin with, the expression $A \to B: \langle m \rangle$ means A sends a message $m$to B.

Step 1: $A \to S: \langle A, B \rangle$

A sends his/her identity and B's identity to the trusted server S as an initial request.

Step 2: $S \to A: \langle Y_A, Y_B \rangle$

After receiving A's request, S chooses two random numbers y_A, $y_B \in Z_q^*$ and computes $Y_A = y_A P + PW_A$ and $Y_B = y_B P + PW_B$, then sends Y_A and Y_B to A.

Step 3: $A \to B: \langle A, X_A, Y_B, \alpha_{AS} \rangle$

When A receives Y_A and Y_B from S, A chooses a random number $x_A \in Z_q^*$ to compute $X_A = x_A P$, $K_{AS} = x_A(Y_A - PW_A)$ and the hash value $\alpha_{AS} = \mathcal{H}(A \Vert S \Vert B \Vert X_A \Vert Y_A \Vert PW_A \Vert K_{AS})$. After computing these values, A sends $\langle A, X_A, Y_B, \alpha_{AS} \rangle$ to B.

Step 4: $B \to S: \langle X_A, X_B, \gamma_B, \alpha_{AS}, \alpha_{BS} \rangle$

After B receives A's messages, B chooses a random number $x_B \in Z_q^*$ to compute $X_B = x_B P$, $K_{BS} = x_B(Y_B - PW_B)$, $K_{AB} = x_B X_A$, and two hash values $\alpha_{BS} = \mathcal{H}(B \Vert S \Vert A \Vert X_B \Vert Y_B \Vert PW_B \Vert K_{BS})$ and $\gamma_B = \mathcal{H}(\text{"1"} \Vert A \Vert S \Vert B \Vert X_A \Vert X_B \Vert K_{AB})$. After computing these values, B sends $\langle X_A, X_B, \gamma_B, \alpha_{AS}, \alpha_{BS} \rangle$ to the server S.

Step 5: $S \to A: \langle X_B, \beta_{AS}, \beta_{BS}, \gamma_B \rangle$

After S receives B's messages, S uses the number chosen in Step 2to compute $K_{AS} = y_A X_A$ and the hash values $\alpha'_{AS} = \mathcal{H}(A \Vert S \Vert B \Vert X_A \Vert Y_A \Vert PW_A \Vert K_{AS})$, and then S verifies the consistency between the computed $\alpha'_{AS}$and the value α_{AS} sent from B. In order to authenticate B, S computes $K_{BS} = y_B X_B$ and the hash value $\alpha'_{BS} = \mathcal{H}(B \Vert S \Vert A \Vert X_B \Vert Y_B \Vert PW_B \Vert K_{BS})$, and then S verifies the consistency between the computed α'_{BS} and the value α_{BS} sent from B. If these values are correct, S computes the hash values $\beta_{AS} = \mathcal{H}(A \Vert S \Vert B \Vert X_A \Vert Y_A \Vert PW_A \Vert K_{AS} \Vert X_B)$ and $\beta_{BS} = \mathcal{H}(B \Vert S \Vert A \Vert X_B \Vert Y_B \Vert PW_B \Vert K_{BS} \Vert X_A)$, and then Ssends $X_B, \beta_{AS}, \beta_{BS}, \gamma_B$ to A.

Step 6: $A \to B: \langle \beta_{BS}, \gamma_A \rangle$

When A receives S's messages, A uses K_{AS}, which was computed in Step 3, and X_B to compute the hash value $\beta'_{AS} = \mathcal{H}(A \Vert S \Vert B \Vert X_A \Vert Y_A \Vert PW_A \Vert K_{AS} \Vert X_B)$. In order to authenticate S, A verifies the consistency between the computed β'_{AS} and the value β_{AS} sent from S. If the result is correct, A computes $K_{AB} = x_A X_B$ and the hash value $\mathcal{H}(\text{"1"} \Vert A \Vert S \Vert B \Vert X_A \Vert X_B \Vert K_{AB})$ and then verifies the value γ_B. If these values are correct, A can make sure that B has the ability to compute the session key $SK = \mathcal{H}(2 \Vert A \Vert S \Vert B \Vert X_A \Vert X_B \Vert K_{AB})$. After that, A sends β_{BS} and γ_A to B.

Step 7:

After receiving A's messages, Bderives the hash value $\mathcal{H}(B \Vert S \Vert A \Vert X_B \Vert Y_B \Vert PW_B \Vert K_{BS} \Vert X_A)$ fromX_A and K_{BS}. In order to authenticate S, B verifies the consistency between β_{BS} and the hash value $\mathcal{H}(B \Vert S \Vert A \Vert X_B \Vert Y_B \Vert PW_B \Vert K_{BS} \Vert X_A)$. If the result is correct, B computes the hash value $\mathcal{H}(\text{"0"} \Vert A \Vert S \Vert B \Vert X_A \Vert X_B \Vert K_{AB})$ and verifies whether the value γ_A which was sent from A is correct or not. If the result is positive, B can make sure that A has ability to compute the session key $SK = \mathcal{H}(2 \Vert A \Vert S \Vert B \Vert X_A \Vert X_B \Vert K_{AB})$.

With the above steps done, A and B can generate a common session key $SK = \mathcal{H}(2 \Vert A \Vert S \Vert B \Vert X_A \Vert X_B \Vert K_{AB})$ via the trusted server S.

3 Some vulnerabilities of Wu et al.'s protocol

In this section, we will show that an off-line guessing attack can break Wu et al.'s protocol. An attacker can pretend to be the server and intercept the messages sent from the users. The structures of the steps of our attack are shown in Figure 2, Figure 3, and Figure 4.

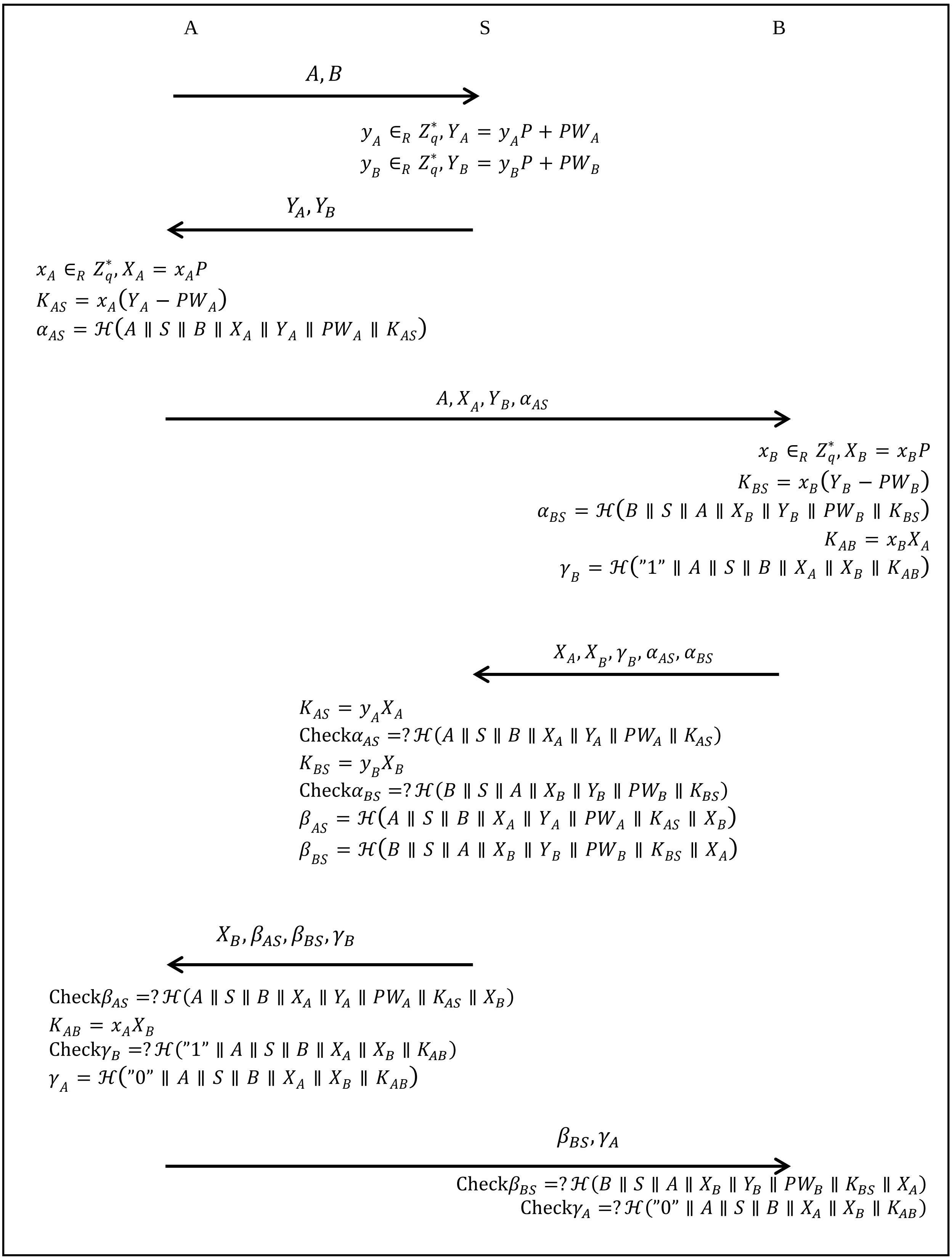

Figure 1: Wu et al.'s 3PAKE protocol

Step 1:

Suppose there is a user A who wants to communicate with another person $\star$. A sends his/her identity along with $\star$'s identity to the server as an initial request. At this point of time, the attacker S^* pretends to be the sever S and intercepts the messages sent from A and

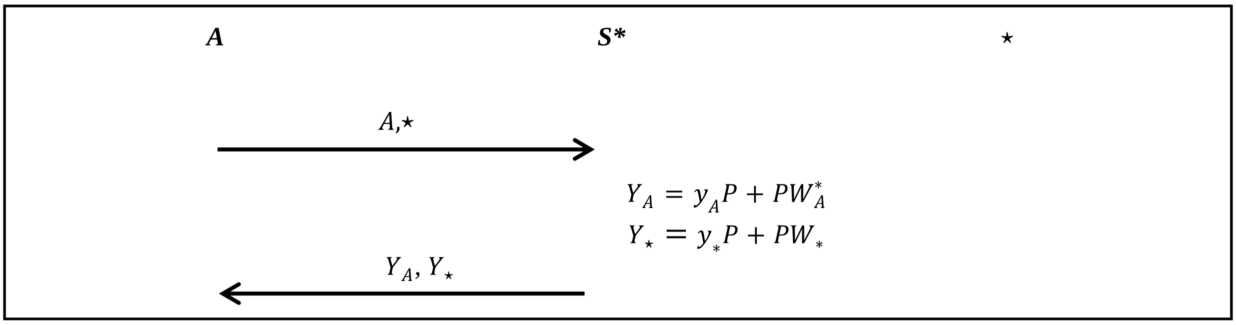

Figure 2: Step 1 of our attack

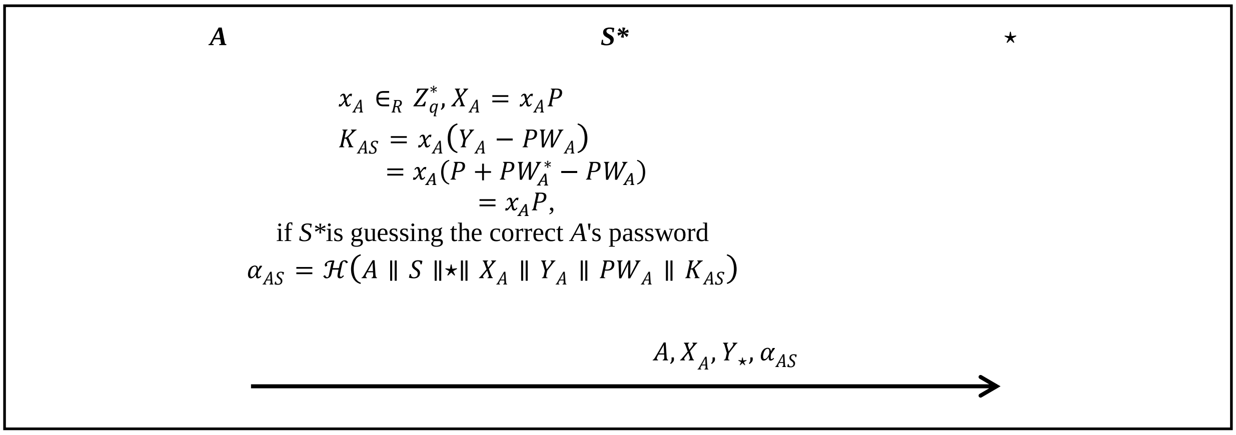

Figure 3: Step 2 of our attack

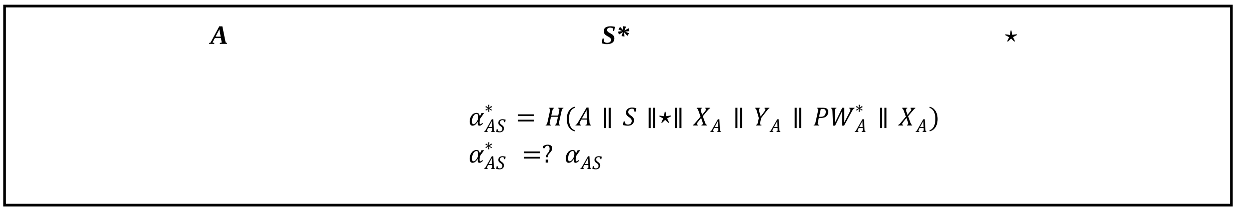

Figure 4: Step 3 of our attack

sets y_A=1 and computes $Y_A = y_A P + PW_A^*$, where PW_A^* is the password which the attacker has guessed. After that, S^* sends Y_A and $Y_\star$ to A, where $Y_\star = y_* P + PW_*$. y_* is a random number and PW_* is a possible password.

Step 2:

When A receives Y_A and $Y_\star$ from S^*, A computes $X_A = x_A P$, $K_{AS} = x_A(Y_A - PW_A)$ and $\alpha_{AS} = \mathcal{H}(A \parallel S \parallel \star \parallel X_A \parallel Y_A \parallel PW_A \parallel K_{AS})$. After finishing the computation, A will send $A, X_A, Y_\star, \alpha_{AS}$ to $\star$. Note that $\mathcal{H}()$ is a public one-way hash function.

Step 3:

When A sends $A, X_A, Y_\star, \alpha_{AS}$ to $\star$, the attacker can intercept the messages and then compute $\alpha_{AS}^* = H(A \parallel S \parallel \star \parallel X_A \parallel Y_A \parallel PW_A^* \parallel X_A)$. If the attacker's guess of the password PW_A^* is correct, then K_{AS} is equal to $x_A P$. The attacker can then use it to compute α_{AS}^* and check if α_{AS}^* is equal to α_{AS}. If it is, the attacker can make sure that he/she has guessed A's password.

4 Improving security of Wu et al.' protocol

To detect the attack during the communication, in Step 3 of Wu et al.'s protocol, A can check to see if X_A is the same as K_{AS}. If it holds, A can be sure that the communication is under attack. In addition, in Step 2 of Wu et al.'s protocol, the server must choose y_A and y_B such that y_A not equal to 1 and y_B not equal to 1.

5 Conclusions

In this paper, we have shown that Wu et al.'s 3PAKE protocol is still vulnerable to the off-line password guessing attack. In addition, we have also offered a simple method to detect the attack.

Acknowledgements

The authors would like to express their appreciation to the anonymous referees for their valuable suggestions and comments. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC 101-2221-E-030-018 and NSC 102-2221-E-030-003.

References

[1] S. M. Bellovin and M. Merritt, “Encrypted key exchange: password-based protocols secure against dictionary attacks,” in Proceedings of 1992 IEEE Computer Society Conference on Research in Security and Privacy, pp. 72-84, 1992.

[2] T. Y. Chang, M. S. Hwang, and W. P. Yang, “A communication-efficient three-party password authenticated key exchange protocol,” Information Sciences, vol. 181, pp. 217-226, 2011.

[3] T. Y. Chang, C. C. Yang and M. S. Hwang, "Improvement of convertible authenticated encryption schemes and its multiple recipients version", International Journal of Security and Its Applications, vol. 6, no. 4, pp. 151-162, 2012.

[4] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password change protocol", Computers & Mathematics with Applications, vol. 49, pp. 703-714, 2005.

[5] T. Y. Chen, C. C. Lee, M. S. Hwang, J. K. Jan, “Towards secure and efficient user authentication scheme using smart card for multi-server environments,” The Journal of Supercomputing, vol. 66, no. 2, pp. 1008-1032, 2013.

[6] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments," International Journal of Network Security, vol. 16, no. 4, pp. 318-321, 2014.

[7] D. He, J. Chen, and J. Hu, “Weaknesses of a remote user password authentication scheme using smart card,” International Journal of Network Security, vol. 13, no. 1, pp. 58-60, 2011.

[8] H. C. Hsiang and W. K. Shih, “Weaknesses and improvements of the Yoon–Ryu–Yoo remote user authentication scheme using smart cards,” Computer Communications, vol. 32, no. 4, pp. 649-652, 2009.

[9] W. B. Hsieh and J. S. Leu, “Exploiting hash functions to intensify the remote user authentication scheme,” Computers & Security, vol. 31, no. 6, pp. 791-798, 2012.

[10] M. S. Hwang, S. Y. Hsiao, W. P. Yang, “Security on improvement of modified authenticated key agreement protocol,” Information - An International Interdisciplinary Journal, vol. 17, no. 4, pp.1173-1178, 2014.

[11] M. S. Hwang, C. C. Lee, Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack", International Journal of Informatica, vol. 12, no. 2, pp.297-302, 2001.

[12] M. S. Hwang, S. K. Chong, T. Y. Chen, “DoS-resistant ID-based password authentication scheme using smart cards”, Journal of Systems and Software, vol. 83, pp. 163-172, 2010.

[13] M. S. Hwang and C. H. Lee, “Authenticated key-exchange in a mobile radio network”, European Transactions on Telecommunications, vo1. 8, no.3, pp.265-269, 1997.

[14] M. S. Hwang, C. W. Lin, C. C. Lee, "Improved Yen-Joye's authenticated multiple-key agreement protocol", IEE Electronics Letters, vol. 38, no. 23, pp. 1429-1431, 2002.

[15] L. C. Huang, M. S. 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.

[16] L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1981.

[17] C. C. Lee, R. X. Chang, and H. J. Ko, “Improving two novel three-party encrypted key exchange protocols with perfect forward secrecy,” International Journal of Foundations of Computer Science, vol. 21, no. 6, pp. 979-991, 2010.

[18] C. C. Lee and Y. F. Chang, “On security of a practical three-party key exchange protocol with round efficiency,” Information Technology and Control, vol. 37, no. 4, pp. 333-335, 2008.

[19] C. C. Lee, S. D. Chen, and C. L. Chen, “A computation-efficient three-party encrypted key exchange protocol,” Applied Mathematics & Information Sciences, vol. 6, no. 3 pp. 573-579, 2012.

[20] C. C. Lee, C. T. Li, and R. X. Chang, “An undetectable on-line password guessing attack on Nam et al.'s three-party key exchange protocol,” accepted to appear in Journal of Computational Methods in Sciences and Engineering, 2013

[21] C. C. Lee, C. T. Li, and C. W. Hsu, “A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps,” Nonlinear Dynamics, vol. 73, no. 1, pp. 125-132, 2013.

[22] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol", International Journal of Network Security, vol. 15, no. 1, pp. 64-67, 2013.

[23] T. F. Lee, J. L. Liu, M. J. Sung, S. B. Yang, and C. M. Chen, “Communication-efficient three-party protocols for authentication and key agreement,” Computers & Mathematics with Applications, vol. 58, no. 4, pp. 641-648, 2009.

[24] T. F. Lee, T. Hwang, and C. L. Lin, “Enhanced three-party encrypted key exchange without server public keys,” Computers & Security, vol. 23, no. 7, pp. 571-577, 2004.

[25] C. T. Li and M. S. Hwang, “An efficient biometrics-based remote user authentication scheme using smart

cards", Journal of Network and Computer Applications, vol. 33, no. 1, pp. 1-5, 2010.

[26] C. T. Li, M. S. Hwang, Y. P. 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, 2008.

[27] C. T. Li, M. S. Hwang, Y. P. 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, 2008.

[28] I-En Liao, C. C. Lee, M. S. Hwang, "A password authentication scheme over insecure networks", Journal of Computer and System Sciences, vol. 72, no. 4, pp. 727-740, 2006.

[29] C. W. Lin, C. S. Tsai, M. S. Hwang, "A new strong-password authentication scheme using one-way hash functions", International Journal of Computer and Systems Sciences, vol. 45, no. 4, pp. 623-626, 2006.

[30] I. C. Lin, H. H. Ou, M. S. Hwang, "A user authentication system using back-propagation network", Neural Computing & Applications, vol. 14, no. 3, pp. 243-249, 2005.

[31] J. W. Lo, J. Z. Lee, M, S. Hwang, Y. P. Chu, "An advanced password authenticated key exchange protocol for imbalanced wireless networks", Journal of Internet Technology, vol. 11, no. 7, pp. 997-1004, 2010.

[32] J. W. Lo, S. C. Lin, M. S. Hwang, "A parallel password-authenticated key exchange protocol for wireless environments", Information Technology and Control, vol. 39, no. 2, pp. 146-151, 2010.

[33] J. J. Shen, C. W. Lin, M. S. Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards", Computers & Security, vol. 22, no. 7, pp. 591-595, 2003.

[34] H. Tao and C. Adams, "Pass-go: aproposal to improve the usability of graphical passwords,"International Journal of Network Security, vol. 7, no. 2, pp. 273-292, 2008.

[35] C. S. Tsai, C. C. Lee, and M. S. Hwang, "Password authentication schemes: current status and key issues,"International Journal of Network Security, vol. 3, no. 2, pp. 101-115, 2006.

[36] R. C. Wang and C. C. Yang, "Cryptanalysis of two improved password authentication schemes using smart cards," International Journal of Network Security, vol. 3, no. 3, pp. 283-285, 2006.

[37] H. C. Wu, M. S. Hwang, C. H. Liu, "A secure strong-password authentication protocol", Fundamenta Informaticae, vol. 68, pp. 399-406, 2005.

[38] S. Wu, Q. Pu, S. Wang, and D. He, "Cryptanalysis of a communication-efficient three-party password authenticated key exchange protocol," *Information Sciences*, vol. 215, pp. 83-96, 2012.

[39] C. C. Yang, T. Y. Chang, M. S. Hwang, "Cryptanalysis of simple authenticated key agreement protocols", IEICE Transactions on Foundations, vol. E87-A, no. 8, pp. 2174-2176, 2004.

[40] Y. Zeng, J. Ma, and M. Sangjae, "An improvement on a three-party password-based key exchange protocol using weil pairing," *International Journal of Network Security*, vol. 11, no. 1, pp. 17-22, 2010.

[41] J. Zhao and D. Gu, "Provably secure three-party password-based authenticated key exchange protocol," *Information Sciences*, vol. 184, no. 1, pp. 310-323, 2012.

[42] Y. Zhang and M. Fujise, "Security management in the next generation wireless networks," *International Journal of Network Security*, vol. 3, no. 1, pp. 1-7, 2006.

[43] X. Zhuang, C. C. Chang, Z. H. Wang, Y. Zhu, "A simple password authentication scheme based on geometric hashing function," *International Journal of Network Security*, vol. 16, no. 4, pp. 237-243, 2014.

Cheng-Chi Lee received the Ph.D. degree in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He is currently an Associate Professor with the Department of Library and Information Science at Fu Jen Catholic University. Dr. Lee is currently as an editorial board member of International Journal of Network Security and Journal of Computer Science. He also served as a reviewer in many SCI-index journals, other journals, other conferences. His current research interests include data security, cryptography, network security, mobile communications and computing, wireless communications. Dr. Lee had published over 100+ articles on the above research fields in international journals.

Shih-Ting Chiu received the B.S. in Computer Science and Information Engineering, National Taitung University, Taitung, Taiwan, R.O.C, in 2012. She will receive the M.S. in Library and Information Science, Fu Jen Catholic University, New Taipei City 24205, Taiwan, R. O. C. Her current research interests include information security and cryptography.

Chun-Ta Li received the Ph.D. degree in Computer Science and Engineering from National Chung Hsing University, Taiwan, in 2008. He is currently an assistant professor of the Department of Information Management, Tainan University of Technology, Tainan, Taiwan. He is a member of IEEE, a member of Chinese Information Security Association, a member of Future Technology Research Association International, a member of IFIP WG 11.3, a member of Machine Intelligence Research Labs, and an editorial board member of International Journal of Network Security. His research interests include information security, wireless sensor networks, mobile computing, and security protocols for ad hoc networks. Dr. Li has published more than 70 papers in international journals and international conferences.