Cryptanalysis of the Tseng-Jan Anonymous Conference Key Distribution System without Using a One-way Hash Function*

Ting-Yi Chang‡ Min-Shiang Hwang† Wei-Pang Yang§

Department of Management Information System†
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw
Fax: 886-4-23742337

Department of Computer and Information Science‡
National Chiao Tung University
1001 Ta Hsueh Road, Hsinchu, Taiwan, R.O.C.
Email: wpyang@cis.nctu.edu.tw

Department of Information Management§
National Dong Hwa University
1, Sec. 2,Da Hsueh Rd., Shou-Feng, Hualien, Taiwan, R.O.C.
Email: wpyang@cis.nctu.edu.tw

November 9, 2004

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-004.

§Responsible for correspondence: Prof. Min-Shiang Hwang

Cryptanalysis of the Tseng-Jan Anonymous Conference Key Distribution System without Using a One-way Hash Function

Abstract

This paper mounts a conspiracy attack on the anonymous conference key distribution system without using a one-way hash function proposed by Tseng and Jan. Our attack can reveal the participant's common key shared by the chairperson.

Keywords: Cryptography, conference key distribution system, user anonymity, one-way hash function, discrete logarithm.

1 Introduction

A conference key distribution system (CKDS) [1, 2, 3, 5] guarantee that all and only participants of the conference share a common conference key which can be used to hold a secure conference. In 1999, Tseng and Jan proposed [4] two CKDSs with user anonymity based on the discrete logarithm problem. One of their schemes requires a one-way hash function to hide identify of the participants and to protect each participant's common key shared by the chairperson. The other scheme does not use a one-way hash function, but it can also achieve the same purposes. Tseng and Jan claimed that both schemes were secure against the impersonation attack and the conspiracy attack. However, this note will point out that the claim made in [4], that their scheme without using a one-way hash function is secure against conspiracy attack, is false.

2 Brief Review of Tseng-Jan CKDS

The scheme includes three stages: (1) system set-up stage, (2) conference key distribution stage, and (3) conference key recovery stage. During the system set-up stage, the system chooses two large primes p and q such that $q \mid (p-1)$ and generates g with order q in $GF(q)$. Then, the system assigns a secret key $x_i \in Z_q^*$ to U_i over a secret channel and publishes the corresponding public key $y_i = g^{xi} \bmod p$.

During the conference key distribution stage, U_c is appointed the chairperson and $A = \{U_1, U_2, \ldots, U_n, n < m\}$ the set of attending members. U_c performs the following steps for distributing a conference key CK shared by the participants in A.

Step 1. Choose a random integer $r \in Z_q^*$ and get a time-sequence T form the system.

Step 2. Compute

$$\begin{aligned} R &= g^r \bmod p, \\ S &= r + H(T \parallel R) \cdot x_c \bmod q. \end{aligned}$$

Here, $H(\cdot)$ denotes a one-way function and $\parallel$ denotes a concatenation.

Step 3. Compute the common secret key shared by each $U_i \in A$ as $k_{ci} = y_i^r \bmod p$.

Step 4. Randomly select a conference key $CK \in Z_q^*$ and construct a polynomial with degree n as

$$\begin{aligned} P(x) &= \prod_{i=1}^{n}(x - k_{ci}) + CK \bmod p, \qquad (1) \\ &= x^n + c_{n-1}x^{n-1} + \cdots + c_0 \bmod p. \end{aligned}$$

Step 5. Broadcast $\{R, S, T, c_{n-1}, c_{n-2}, \ldots, c_0\}$.

During the conference key recovery stage, each $U_i \in A$ receives $\{R,\ S,\ T,\ c_{n-1},\ c_{n-2},\ \cdots,\ c_0\}$ and performs the following steps for recovering the conference key CK.

Step 1. Verify T and the following equation

$$g^S = R \cdot y_c^{H(T\|R)} \bmod p.$$

Step 2. Compute the common secret key shared with U_c as $k_{ic} = R^{x_i} \bmod p$.

Step 3. Recover CK by computing

$$\begin{aligned} P(k_{ic}) &= (k_{ic})^n + c_{n-1}(k_{ic})^{n-1} + \cdots + c_1 k_{ic} + c_0 \bmod p, \\ &= CK \bmod p. \end{aligned}$$

3 The Weakness of Tseng-Jan Scheme

Tseng and Jan claimed that their conference key distribution system was secure against the conspiracy attack. However, in this section, we will show that the participant's common secret key shared with the chairperson can be revealed by the conspiracy attack. Any $(n-1)$ attending members in A can conspire to reveal the only other member's common secret key shared with the chairperson.

For example, assume that $(n-1)$ attending members U_i $(i = 1, 2, \ldots, n-1)$ intend to reveal the other member U_n's common secret key k_{cn}. After substituting x to zero in Equation (1), we can obtain the equation $\prod_{i=1}^{n-1}(-k_{ci}) \times (-k_{cn}) = c_0 - CK \bmod p$. With the knowledge of the values c_0, CK and $\prod_{i=1}^{n-1}(-k_{ci})$, the common secret key k_{cn} can be computed. Thus, any $(n-1)$ attending members $U_1, U_2, \ldots, U_{n-1}$ can easily reveal U_n's common secret key k_{cn} shared with the chairperson U_c. Though k_{cn}, shared between U_c and U_n, is different in the next conference, if U_c and U_n use it to communicate with each other in this conference, $U_1, U_2, \ldots, U_{n-1}$ can eavesdrop the confidential message between them.

4 Conclusion

In this paper, we have shown that Tseng and Jan's claim, that their conference key distribution system is secure against the conspiracy attack, is false. Any

$(n-1)$ attending members can conspire to reveal the only other member's common secret key shared with the chairperson.

References

[1] S. Hirose and K. Ikeda, "A conference distribution system for the start configuration based on the discrete logarithm problem," *Information Processing Letters*, vol. 62, no. 4, pp. 189–192, 1997.

[2] Min-Shiang Hwang and W. P. Yang, "Conference key distribution protocols for digital mobile communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 13, pp. 416–420, Feb. 1995.

[3] I. Ingemaresson, T. D. Tang, and C. K. Wong, "A conference key distribution system," *IEEE Transactions on Information Theory*, vol. 28, no. 5, pp. 714–720, 1982.

[4] Yuh-Min Tseng and Jinn-Ke Jan, "Anonymous conference key distribution systems based on the discrete logarithm problem," *Computer Communications*, vol. 22, no. 8, pp. 749–754, 1999.

[5] T. C. Wu, "Conference key distribution system with uesr anonymity based on algebraic approach," *IEE Proceedings - Computer Digital Technology*, vol. 144, no. 2, pp. 145–148, 1997.

BIOGRAPHY

Ting-Yi Chang received the B.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2001, and his M.S. in Department and Graduate Institute of Computer Science and Information Engineering from CYUT, in 2003. He is currently pursuing his Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, Republic of China. His current research interests include information security, cryptography, and mobile communications.

Min-Shiang Hwang was born on August 27, 1960 in Tainan, Taiwan, Republic of China (ROC.). He 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. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Outstanding Research Award of National Science Council of the Republic of China. He is currently a professor of the department of Management Information Systems, National Chung Hsing University, Taiwan, ROC. 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 over 100 articles on the above research fields in international journals.

Wei-Pang Yang was born on May 17, 1950 in Hualien, Taiwan, Republic of China. He received the B.S. degree in mathematics from National Taiwan Normal University in 1974, and the M.S. and Ph.D. degrees from the National Chiao Tung University in 1979 and 1984, respectively, both in computer engineering. Since August 1979, he has been on the faculty of the Department of Computer Engineering at National Chiao Tung University , Hsinchu, Taiwan. In the academic year 1985-1986, he was awarded the National Postdoctoral Research Fellowship and was a visiting scholar at Harvard University. From 1986 to 1987, he was the Director of the Computer Center of National Chiao Tung University. In August 1988, he joined the Department of Computer and Information Science at National Chiao Tung University, and acted as the Head of the Department for one year. Then he went to IBM Almaden Research Center in San Jose, California for another one year as visiting scientist. From 1990 to 1992, he was the Head of the Department of Computer and Information Science again. His research interests include database theory, database security, object-oriented database, image database and Chinese database systems. Dr. Yang is a full professor and a member of IEEE, ACM, and the phi Tau Phi Society. He was the winner of the 1988 and 1992 Acer Long Term Award for Outstanding M.S. Thesis Supervision, and the winner of 1990 Outstanding Paper Award of the Computer Society of the Republic of China. He also obtained the 1991-1993 Outstanding Research Award of National Science Council of the Republic of China.