CRYPTANALYSIS OF THE TSENG-JAN ANONYMOUS CONFERENCE KEY DISTRIBUTION SYSTEM WITHOUT USING A ONE-WAY HASH FUNCTION

Ting-Yi CHANG, Min-Shiang HWANG, and Wei-Pang YANG

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. The attack described in the article can reveal the participants' common key shared with the chairperson.

Keywords: Cryptography, Conference Key Distribution System, User Anonymity, One-way Hash Function, Discrete Logarithm.

A Conference Key Distribution System (CKDS) [1,2,3,4] guarantees that all and only the participants in a conference share a common conference key which can be used to hold a secure conference. In 1999, Tseng and Jan proposed two CKDSs with user anonymity based on the discrete logarithm problem.[5] One of their schemes requires a one-way hash function to hide the identity of the participants and to protect each participant's common key shared with the chairperson. The other scheme does not use a one-way hash function, but it can also achieve the same purposes. Tseng and Jan claim that both schemes are secure against the impersonation attack and the conspiracy attack. However, this paper will demonstrate that the claim made by Tseng and Jan,[6] that their scheme without using a one-way hash function is secure against conspiracy attack, is incorrect.

Brief Review of Tseng-Jan's Conference Key Distribution System

The conference key distribution scheme proposed by Tseng and Jan includes three stages:

- System set-up stage,
- Conference key distribution stage, and

- 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 of order q in $GF(q)$. Then, the system assigns a secret key $x_i \in Z_q^*$ to user U_i over a secret channel and publishes the corresponding public key $y_i = g^{x_i} \bmod p$.

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

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

Step 2. Compute

$$R = g^r \bmod p$$
$$S = r + H(T \,||\, R) \cdot x_c \bmod q$$

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

Step 3. Compute the common secret key for 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 of degree n as

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

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 $\{R, S, T, c_{n-1}, c_{n-2}, \ldots, c_0\}$ 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

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

The Weakness of Tseng-Jan's Scheme

Tseng and Jan claim that their conference key distribution system is secure against the conspiracy attack. However, in this section, we will show that the participants' common secret key shared with the chairperson can be revealed with the conspiracy attack. Any $(n-1)$ attending members in A can conspire in order to reveal the remaining 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 remaining other member U_n's common secret key k_{cn}. After substituting x with zero in Equation 1, we can obtain the equation:

$$\prod_{i=1}^{n-1}(-k_{ci}) \times (-k_{cn}) = c_0 - CK \bmod p .$$

Knowing 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 at the next conference, if U_c and U_n use it to communicate with each other at this conference, $U_1, U_2, \ldots, U_{n-1}$ can eavesdrop confidential information exchanged between them.

Conclusion

In this article, the authors have shown that Tseng and Jan's claim that their conference key distribution system is secure against the conspiracy attack is wrong. Any $(n-1)$ attending members can conspire to reveal the remaining other member's common secret key shared with the chairperson.

Acknowledgment

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

Notes:

---

[1] Shouichi Hirose and Katsuo Ikeda, "A Conference Distribution System for the Star Configuration Based on the Discrete Logarithm Problem," *Information Processing Letters* 62, no. 4 (May 1997): 189-192.

[2] Min-Shiang Hwang and Wei-Pang Yang, "Conference Key Distribution Protocols for Digital Mobile Communication Systems," *IEEE Journal on Selected Areas in Communications* 13, no. 2 (February 1995): 416-420.

[3] Ingemar Ingemarsson, Donald T. Tang, and C.K. Wong, "A Conference Key Distribution System," *IEEE Transactions on Information Theory* 28, no.5 (September 1982): 714-720.

[4] T.C. Wu, "Conference Key Distribution System with User Anonymity Based on Algebraic Approach," *IEE Proceedings – Computers and Digital Techniques* 144, no. 2 (March 1997): 145-148.

[5] Yuh-Min Tseng and Jinn-Ke Jan, "Anonymous Conference Key Distribution Systems Based on the Discrete Logarithm Problem," *Computer Communications* 22, no. 8 (1999): 749-754.

[6] Tseng and Jan, "Anonymous Conference Key Distribution Systems Based on the Discrete Logarithm Problem."

TING-YI CHANG received a B.S. degree in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2001, and a M.S. degree from the Department and Graduate Institute of Computer Science and Information Engineering of CYUT, in 2003. He is currently pursuing his Ph.D. in Computer and Information Science from the National Chiao Tung University, Taiwan, Republic of China. His current research interests include information security, cryptography, and mobile communications. *Address for correspondence:* Department of Computer and Information, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu, Taiwan, R.O.C. *Email:* wpyang@cis.nctu.edu.tw.

MIN-SHIANG HWANG see page 20

WEI-PANG YANG was born on May 17, 1950 in Hualien, Taiwan, Republic of China. He received a B.S. degree in Mathematics from the National Taiwan Normal University in 1974, and a M.S. and a Ph.D. degrees from the National Chiao Tung University in 1979 and 1984, respectively, both in Computer Engineering. Since August 1979, he has been a member of the faculty of the Department of Computer Engineering at National Chiao Tung University, Hsinchu, Taiwan. In the academic year 1985-1986, he was awarded a National Postdoctoral Research Fellowship and was a visiting scholar at the Harvard University. From 1986 to 1987, he was Director of the Computer Center of the National Chiao Tung University. In August 1988, he joined the Department of Computer and Information Science at the National Chiao Tung University, and acted as Head of the Department for one year. Then, he joined IBM's Almaden Research Center in San Jose, California for another year as a visiting scientist. From 1990 to 1992, he was again Head of the Department of Computer and Information Science. His research interests include database theory, database security, object-oriented databases, image databases and Chinese database systems. Dr. Yang is a full professor and a member of IEEE, ACM, and the 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 the National Science Council of the Republic of China. *Address for correspondence:* 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.