Cryptanalysis of Liaw's Broadcasting Cryptosystem

YUH-MIN TSENG*
Department of Information Management
Nan-Kai College of Technology and Commerce
Nantou, Taiwan 542, R.O.C.
ty@bear.nkjc.edu.tw

JINN-KE JAN
Institute of Applied Mathematics, National Chung Hsing University
Taichung, Taiwan 402, R.O.C.
jkjan@amath.nchu.edu.tw

(Received August 1999; revised and accepted April 2000)

Abstract—In 1999, Liaw proposed a new broadcasting cryptosystem, which requires smaller bandwidth as compared to the previously proposed broadcasting cryptosystems. However, this article will show that the proposed system is insecure enough by presenting a conspiracy attack on it. We will also point out some ambiguous problems in Liaw's paper. Moreover, we propose an improved broadcasting cryptosystem, which is a slight modification of the proposed system to overcome the conspiracy attack. © 2001 Elsevier Science Ltd. All rights reserved.

Keywords—Cryptography, Broadcasting cryptosystem, Cryptanalysis.

1. INTRODUCTION

Communication techniques have encouraged the distribution of information. How to establish secure and efficient communications among users over insecure computer networks is important. One of the important issues for achieving the aforementioned requirements is the development of the broadcasting cryptosystem. The broadcasting cryptosystem is that a sender can broadcast an encrypted message and only certain authorized subsets in the system can decrypt the message. Based upon cryptographic techniques, several broadcasting cryptosystems [1-3] have been proposed. However, the previously proposed cryptosystems [1,2] need many broadcasting messages, and it is hard to insert new users into the system. To remedy the drawbacks, Liaw [3] proposed a new broadcasting cryptosystem based on the RSA scheme [4] and a symmetric cryptosystem (e.g., DES [5]).

First, we will review and point out some ambiguous problems in Liaw's paper [3]. It is beneficial to read his paper. Moreover, one conspiracy attack is given in this paper to show that Liaw's
broadcasting cryptosystem is not secure enough. We are going to show that two users can collaborate to derive the secret key of the central authority server. In such cases, the secret keys of all users in the system will be also revealed. The two users can always decrypt any transmitted ciphertexts in the system, even though the transmitted messages are not authorized for them. Therefore, we also propose a slight modification of Liaw’s broadcasting cryptosystem to enhance the level of security.

2. REVIEW AND AMBIGUOUS PROBLEMS OF LIAW’S BROADCASTING SYSTEM

Here, we review briefly Liaw’s broadcasting cryptosystem. Meanwhile, we also point out some ambiguous problems in it. In the system, there is a central authority server (CAS for short). The CAS is responsible for generating the system parameters and the keys for all users $U_i$ ($i = 1, 2, \ldots, n$). Initially, the CAS secretly chooses two large strong primes $p = 2p' + 1$ and $q = 2q' + 1$, where $p'$ and $q'$ are also primes [6,7], and then publishes $N = pq$. Define $\lambda(N) = \text{lcm}(p - 1, q - 1)$ and select a public key $d$ such that $ed \equiv 1 \mod \lambda(N)$, where $\Phi$ denotes the Euler totient function [8] and $e$ denotes the secret key of the system. Note that the above parameters have some slight modifications as compared to ones of the RSA system. Also, the CAS publishes a secure symmetric cryptosystem that $E(.)$ is the encryption algorithm and $D(.)$ is the corresponding decryption algorithm. Therefore, $M = D_{MK}(E_{MK}(M))$, where $MK$ is the encryption/decryption key for the symmetric cryptosystem. Then, the CAS selects a secret key $K_0$ and computes each user $U_i$’s secret keys $t_i$ and $K_i$, and the public key $f(t_i)$ as follows:

$$K_i = K_0^t_i \mod N, \quad \text{and} \quad f(t_i) = t_i^e,$$

where each $t_i$ is a prime number selected by the CAS. Note that all $t_i$ are distinct odd primes and different from $p'$ and $q'$.

During the broadcasting encryption phase, without loss of generality, suppose that the sender $U_1$ wants to broadcast a message $M$ to the legitimate receivers $U_2, U_3, \ldots, U_a$ secretly, and $U_{a+1}, U_{a+2}, \ldots, U_n$ are illegitimate receivers. $U_1$ and CAS perform the following encryption steps to generate the ciphertext for $M$.

STEP 1. $U_1$ calls the CAS that he wants to broadcast a message to $U_2, U_3, \ldots, U_a$.

STEP 2. CAS computes two public keys $f(B_1)$ and $PK_1$ as follows:

$$B_1 = t_2 \times t_3 \times \cdots \times t_a, \quad f(B_1) = B_1^e, \quad MK_1 = K_0^{B_1} \mod N, \quad PK_1 = E_{t_1}(MK_1).$$

STEP 3. Upon receiving $f(B_1)$ and $C$, $U_1$ recovers $MK_1 = D_{t_1}(PK_1)$ and broadcasts the ciphertext $C = E_{MK_1}(M)$.

As mentioned above, there is a matter needs to be cleared up. Is the public key $f(t_i)$ equal to $t_i^e$ as an integer or $t_i^e \mod \lambda(N)$? If $t_i^e$ is computed in $Z$, the system is completely insecure for the following reason: An attacker can find the system’s secret key $e$ and factor $N$, since $d$ is public and he may find $de - 1$ which is multiple of $\lambda(N)$. Therefore, it must be $t_i^e \mod \lambda(N)$. For the same reason, $B_1$ and $f(B_1)$ are also to be reduced mod $\lambda(N)$.

During the decryption phase, only the legitimate receivers $U_j$ ($j = 2, 3, \ldots, a$) may obtain the message $M$ after receiving $f(B_1)$ and $C$. Each legitimate receiver $U_j$ uses his own secret key $K_j$ to obtain the encryption/decryption key $MK_1$ by computing $K_j^{(f(B_1)/f(t_j))^d} \mod N$.

Note that since $U_j$ does not know $\lambda(N)$ and he must compute $K_j^{(f(B_1)/f(t_j))^d} \mod N$, this will force $d$ to be short. Otherwise, it is time-consuming. We suggest that the size of $d$ should be 16 bits. Thus, this will not impair the security of the system [9].
3. CRYPTANALYSIS

In this section, we will show that any two users in Liaw’s system can cooperatively derive the CAS’s secret key $K_0$ by the Euclidean algorithm [8]. Meanwhile, the secret key for each user in the system will also be revealed.

Let $U_x$ and $U_y$ be two arbitrary users in the system. Since, the secret key $K_x$ of $U_x$ is computed by $K_x = K_t^t_x \mod N$, $t_x$ is also another secret key of $U_x$. Because all $t_i$ are distinct odd primes and different from $p'$ and $q'$, it is obvious that $t_x$ of $U_x$ and $t_y$ of $U_y$ are relatively prime. Therefore, $U_x$ and $U_y$ can collude to find two numbers $r$ and $s$ that satisfy $rt_x + st_y = 1$ by the Euclidean algorithm. Thus, the CAS’s secret key $K_0$ can be computed as follows:

$$K_x^r K_y^s \mod N = K_0^{rt_x} K_0^{st_y} \mod N = K_0^{rt_x + st_y} \mod N = K_0 \mod N.$$ 

In this case, the secret key $K_j$ of each user $U_j$ in the system can also be revealed by computing

$$K_0^{f(t_j)^d} \mod N = K_0^{rt_x \mod \lambda(N)} \mod N = K_0^t \mod N = K_j \mod N,$$

where $f(t_j) = t_j^r \mod \lambda(N)$ is the public key of $U_j$ and $d$ is the public key of CAS.

As stated above, the proposed system is vulnerable to the conspiracy attack. That is, two cooperative users can always decrypt any transmitted ciphertexts in the system, even though they are not the legitimate receivers.

4. MODIFICATIONS

We have shown that Liaw’s system is insecure. From the above cryptanalysis, we see that $U_x$ and $U_y$ can use their secret keys $t_x$ and $t_y$ to derive the CAS’s secret key $K_0$ cooperatively. Therefore, $t_x$ and $t_y$ should only be possessed by the CAS so that the secret key for each user $U_i$ is only $K_i$. In such cases, Steps 2 and 3 in the broadcasting encryption phase need to be modified, and the other phases remain unchanged. The detailed modifications are presented as follows.

*STEP 2.* CAS computes two public keys $f(B_1)$ and $PK_1$ as follows:

$$B_1 = t_2 \times t_3 \times \cdots \times t_a \mod \lambda(N), \quad f(b_1) = B_1^f \mod \lambda(N),
MK_1 = K_0^{B_1} \mod N, \quad PK_1 = E_{K_1}(MK_1).$$

*STEP 3.* Upon receiving $f(B_1)$ and $PK_1$, $U_1$ recovers $MK_1 = D_{K_1}(PK_1)$ and broadcasts the ciphertext $C = E_{MK_1}(M)$.

During the decryption phase, each legitimate receiver $U_j$ only adopts his own secret key $K_j$ and public key $f(t_j)$ to obtain the encryption/decryption key $MK_1$ by computing $K_j^{f(B_1)/f(t_j)^d} \mod N$. In fact, we can see that the secret value $t_j$ for each user $U_j$ in Liaw’s system does not need to be possessed by each user $U_j$.

5. DISCUSSIONS

In the improved system, although $f(t_i) = t_i^r \mod \lambda(N)$ is the public key of a user $U_i$, an adversary or $U_i$ does not know the value $\lambda(N)$, so that they cannot obtain $t_i$. Since $t_i$ is unknown, any two users $U_x$ and $U_y$ cannot collude to derive the CAS’s secret key $K_0$ by adopting the Euclidean algorithm to find two numbers $r$ and $s$ such that $rt_x + st_x = 1$ as the cryptanalysis mentioned in Section 3. Therefore, the modified system not only retains the advantages of Liaw’s system, but also prevents the conspiracy attack.
REFERENCES


