

Cryptanalysis of Improved Liaw's Broadcasting Cryptosystem*

J. MUÑOZ MASQUÉ AND A. PEINADO**

*Departamento de Tratamiento de la Información y Codificación
Instituto de Física Aplicada del CSIC
C/Serrano, 144 – 28006 Madrid, Spain
E-mail: jaime@iec.scic.es*

***Departamento de Ingeniería de Comunicaciones
E.T.S.I. Telecomunicación
Universidad de Málaga
Campus de Teatinos, E29071 Málaga, Spain
E-mail: apeinado@ic.uma.es*

An inconsistency in the improvement given in [1] on Liaw's broadcasting cryptosystem [2] is detected and new attacks to the system are presented. A modification of the cryptosystem to overcome both the conspiracy attack and our own cryptanalysis is proposed.

Keywords: cryptanalysis, broadcasting encryption, key management, public-key cryptosystem, eavesdropping, factorization problem

1. INTRODUCTION

A secure broadcasting cryptosystem must provide a secure communication channel from a sender to a group of legal or authorized receivers. Many of the proposed systems [3-5] require a large number of broadcast messages and present a number of problems. Moreover, Liaw [2] proposed a secure broadcasting scheme with fewer broadcasting messages, which allows easy insertion of new users into the active group. Later, Tseng and Jan [1] found several weaknesses in Liaw's scheme and proposed a modification. The weaknesses detected in [1] allow intruders to obtain the master key by means of a conspiracy attack, thus breaking the security of the system. Moreover, Sun [7] proved that Liaw's broadcasting cryptosystem cannot be operated because a very large amount of information ($\sim 2^{71}$ bits) must be kept by each user and be sent for each broadcast.

In the present paper, an inconsistency in the improvement proposed by Tseng and Jan in [1] is detected precluding its application. New attacks on the original and modified Liaw's schemes [1, 2] are presented and a new modification is proposed which overcomes the conspiracy attack of Tseng and Jan. We also give our own cryptanalysis. This modification does not require keeping and broadcasting the very large amount of information pointed out in [7].

Received June 16, 2003; revised October 7, 2004 & March 10, 2005; accepted September 26, 2005.

Communicated by Shih-Pyng Shieh.

* This work has been supported by MEC-Spain under grant SEG2004-02418, "Evaluación de protocolos y algoritmos de seguridad en sistemas de información."

2. LIAW'S BROADCASTING CRYPTOSYSTEM

This paper uses the same notations as in [1, 2], thus differentiating three phases in the protocol. We consider a system composed of a central authority server (CAS) and n users U_i , $1 \leq i \leq n$.

System setup phase. In this first phase, a central authority server (CAS) generates the public and private keys for every user U_i in the system and defines the following system parameters. Let $N = pq$ be an RSA modulus [9] where $p = 2p' + 1$, $q = 2q' + 1$, are safe prime numbers, *i.e.*, p, q, p', q' are all prime. We set $\lambda(N) = \text{lcm}(p-1, q-1)$ and denote the Euler totient function by $\phi(N)$. Integers d, e are selected such that $de \equiv 1 \pmod{\phi(\lambda(N))}$ and are the public key and private key of the system, respectively. Hence, N and d are made public, whereas p, q and e are kept secret. Next, CAS chooses a secret integer K_0 and computes the private key (t_i, K_i) and the public key $f(t_i)$ for every user U_i such that

$$\begin{aligned} K_i &= K_0^{t_i} \pmod{N}, \\ f(t_i) &= t_i^e, \end{aligned} \tag{1}$$

where t_i is prime. Note that no modular operation is performed when computing $f(t_i)$.

Broadcasting phase. When a user U_1 wants to broadcast a message to users U_2, \dots, U_a , the CAS is informed and computes

$$\begin{aligned} f(B_1) &= B_1^e, \\ MK_1 &= K_0^{B_1} \pmod{N}, \\ PK_1 &= E_{t_1}(MK_1), \end{aligned} \tag{2}$$

where $B_1 = t_2 t_3 \dots t_a$ and $E_k(\cdot)$ is the symmetric encryption function of the system with key k . No modulus operation is performed when computing $f(B_1)$. Next, CAS sends $f(B_1)$ and PK_1 to user U_1 , and $f(B_1)$ to every user U_i , $2 \leq i \leq a$. Accordingly, U_1 can safely recover the secret key

$$MK_1 = D_{t_1}(PK_1), \tag{3}$$

and encipher the message M as

$$C = E_{MK_1}(M), \tag{4}$$

and then broadcast C .

Decryption phase. When a legal user U_j , $2 \leq j \leq a$, receives $f(B_1)$ and C , the secret key is obtained by computing

$$\begin{aligned}
MK_1 &= K_j^{(f(B_1)/f(t_j))^d} \bmod N = K_0^{t_j \left(\prod_{i \neq j, 2 \leq i \leq a} t_i^e \right)^d} \bmod N \\
&= K_0^{t_2 t_3 \dots t_a} \bmod N = K_0^{B_1} \bmod N,
\end{aligned} \tag{5}$$

and, hence, the message M is deciphered. Note that no modulus operation can be applied over the exponent to reduce the computational cost because the users do not know $\phi(\lambda(N))$.

3. ANALYSIS OF THE IMPROVED LIAW'S BROADCASTING CRYPTOSYSTEM

The modifications proposed in [1] by Tseng and Jan can be summarized as follows:

- a) The private key t_j must only be known to CAS. Therefore, the private key and public key of every user U_j will be K_j and $f(t_j)$, respectively. In this way, the conspiracy attack to obtain K_0 cannot be performed since U_j does not know his own t_j .
- b) The function f is now defined as $f(x) = x^e \bmod \lambda(N)$, rather than $f(x) = x^e$. Hence, the public key $f(t_i)$ of user U_i and $f(B_1)$ are computed as

$$\begin{aligned}
f(t_i) &= t_i^e \bmod \lambda(N), \\
f(B_1) &= (t_2 t_3 \dots t_a)^e \bmod \lambda(N).
\end{aligned} \tag{6}$$

The rest of operations remain unchanged and the system works following the previous (original) scheme.

We agree with [1] that publishing the values $f(t_i) = t_i^e$ compromises the security of Liaw's cryptosystem since, though factoring integers is a hard problem, detecting whether a given integer is a prime power is not that hard. In fact, if $k = \pi^e$, π being a prime, then by Fermat's theorem we have

$$b^k = (F \circ \dots \circ F)(b) \equiv b \pmod{\pi}, \tag{7}$$

for every integer b , where F is the function defined by $F(x) = x^\pi$.

Hence, π divides $\gcd(b^k - b, k)$ and for most values of b we will even have $\gcd(b^k - b, k) = \pi$.

As the running time for the Euclid algorithm is $O((\ln k)^2)$ and computing $b^k \pmod{k}$ is $O((\ln k)^2 \ln b)$, it follows that $k = \pi^e$ can be factored in $O((\ln k)^3)$; for example, see [6, Algorithm 1.7.4]. This factorization problem is also taken into account in [7] in order to state the minimum bit length of t_i , making the system computationally safe.

According to [1], the value to be published must be $f(t_i) = t_i^e \bmod \lambda(N)$, rather than $f(t_i) = t_i^e$ itself. The problem is that, in this case, Theorem 1 in [2] is no longer true. Actually, as simple numerical examples show, the quotient $f(B_1)/f(t_i)$ may not be an integer and hence the decryption process could fail. The procedure to recover the key MK_1 as explained in [1] is not valid as the quotient $f(B_1)/f(t_i)$ does not exist in Z . As a conse-

quence, the modification proposed in [1] cannot be regarded as an improvement of the system in [2]. In section 5, a modification is presented to solve the inconsistency and to overcome the attacks in [1].

4. NEW ATTACKS ON LIAW'S BROADCASTING CRYPTOSYSTEM

In addition to the conspiracy attack presented in [1], there are other aspects that can compromise the security of Liaw's original cryptosystem.

First attack. Assume user U_1 wants to broadcast a message to the group of users $\{U_2, U_3, \dots, U_a\}$. Accordingly, the CAS will generate the key $MK_1 = K_0^{B_1} \bmod N$, with $B_1 = t_2 \dots t_a$. Then, assuming that user $U_{a+1} \notin \{U_1, U_2, \dots, U_a\}$ wants to broadcast a message to the same group of users the CAS will generate the key

$$MK_{a+1} = K_0^{B_{a+1}} \bmod N, \quad (8)$$

with $B_{a+1} = t_2 \dots t_a$. As is evident, the values MK_{a+1} and B_{a+1} are identical to those generated for U_1 , namely, MK_1 and B_1 . This implies that user U_{a+1} , who is not authorized, can read the messages from U_1 to the group $\{U_2, U_3, \dots, U_a\}$, and conversely.

Second attack. The first attack can be generalized in the following way. Assume U_{a+1} wants to broadcast a message to the group of users $\{U_2, U_3, \dots, U_a, U_{a+2}, U_{a+3}, \dots, U_b\}$, which includes the group of legitimate receivers for U_1 , i.e., $\{U_2, U_3, \dots, U_a\}$. In this case, CAS will generate

$$\begin{aligned} B_{a+1} &= t_2 t_3 \dots t_a t_{a+2} \dots t_b, \\ f(B_{a+1}) &= B_{a+1}^e, \\ MK_{a+1} &= K_0^{B_{a+1}} \bmod N. \end{aligned} \quad (9)$$

Then, unauthorized user U_1 can recover the new key MK_{a+1} , as follows:

$$MK_1^{f(t_{a+2})^d f(t_{a+3})^d \dots f(t_b)^d} \bmod N = K_0^{t_2 t_3 \dots t_a t_{a+2} \dots t_b} \bmod N = MK_{a+1}. \quad (10)$$

Therefore, every user U_j of the system, who formerly sent a message to a group of users GU_1 , can decrypt the messages that a third user $U_k \notin GU_1 \cup \{U_1\}$ sends to a distinct group GU_2 whenever $GU_1 \subseteq GU_2$.

Third attack. There is a particular case in which Liaw's cryptosystem fails. Assume the user U_1 asks the CAS to send a message to a unique user U_2 . This is not a common use of the cryptosystem as it is designed to broadcast messages to a group of users, but this option is permitted by the system. In such a case, the CAS would generate the following parameters:

$$B_1 = t_2, \quad (11)$$

$$f(B_1) = B_1^e = t_2^e,$$

$$MK_1 = K_0^{B_1} \bmod N = K_0^{t_2} \bmod N = K_2.$$

In this way, U_1 will directly know the private key K_2 of the user U_2 , compromising the security of the system.

It is important to note that these attacks are also applicable to the case in which B_i and $f(B_i)$ are computed by applying modulus $\lambda(N)$ reduction, as proposed in [1].

5. MODIFICATIONS TO THE ORIGINAL SCHEME

In order to solve the new weaknesses presented in the previous section, as well as the conspiracy attack in [1], we propose including the following modifications to Liaw's broadcasting cryptosystem.

- a) According to [1], the prime numbers t_j will only be known to the CAS; even user U_j will not know its value. In this way, the weakness pointed out in [7] related to the reconstruction of K_0 from the knowledge of t_j has no effect on this scheme.
- b) According to [1], the function f is redefined as $f(x) = x^e \bmod \lambda(N)$. Hence, we have

$$f(t_j) = t_j^e \bmod \lambda(N), \quad (12)$$

$$f(B_i) = B_i^e \bmod \lambda(N).$$

By means of this modification, the weakness in [7] regarding the factorization is no longer present, and the amount of information to be kept or sent is not so large as those suggested in [7]. In section 6, more details regarding this topic will be given.

- c) The parameter B_1 generated by CAS will also include the parameter t_1 of the user U_1 who wishes to send a message to the group of users $GU_1 = \{U_2, U_3, \dots, U_a\}$. Hence, we have

$$B_1 = t_1 t_2 \dots t_a \bmod \lambda(N). \quad (13)$$

This modification thwarts the attacks in section 4.

- d) The modification b) forces the receivers to modify the key reconstruction algorithm because the value $f(B_i)/f(t_j)$ is not always an integer. Hence, the CAS computes $f(r_c/t_j)$ instead of $f(t_j)$, where r_c is a random integer chosen by CAS. A legal user U_j can reconstruct the key as

$$MK_1 = K_j^{f(B_1)^d \cdot f(r_c/t_j)^d} \bmod N \quad (14)$$

$$= K_0^{t_1 t_2 \dots t_a r_c} \bmod N$$

$$= K_0^{B_1 r_c} \bmod N.$$

More precisely, assuming that U_1 wants to broadcast a message to the group of users

$GU_1 = \{U_2, U_3, \dots, U_a\}$, then U_2 can reconstruct the key MK_1 as

$$\begin{aligned} MK_1 &= K_2^{f(B_1)^d \cdot f(r_c/t_2)^d} \bmod N \\ &= K_0^{t_1 t_2 \dots t_a r_c} \bmod N \\ &= K_0^{B_1 r_c} \bmod N. \end{aligned} \quad (15)$$

Note that no modular operation can be applied to the exponent in Eqs. (14) - (15) because the users do not know the value of $\lambda(N)$. This fact implies that the enciphering (public) exponent d must be short.

e) Furthermore, the CAS is not required to compute and send PK_1 to user U_1 (see Eq. (2)), as U_1 can obtain the key MK_1 in the same way as the legitimate receivers, *i.e.*,

$$\begin{aligned} MK_1 &= K_1^{f(B_1)^d \cdot f(r_c/t_1)^d} \bmod N \\ &= K_0^{t_1 t_2 \dots t_a r_c} \bmod N \\ &= K_0^{B_1 r_c} \bmod N. \end{aligned} \quad (16)$$

All these modifications allow us to redefine Liaw's broadcasting cryptosystem according to the following steps and phases.

Phase 1: System setup phase. This phase results from applying previous modifications a) and b) to the original setup phase defined in [1, 2]. In other words, CAS chooses p , q , and r_c , and computes the system parameters $N = pq$, and e , d such that $ed \equiv 1 \pmod{\lambda(N)}$. Then, CAS chooses the system key K_0 and the prime numbers t_j , and computes private key K_i and public key $f(r_c/t_j)$ for every user U_i in the system by

$$\begin{aligned} K_i &= K_0^{t_i} \bmod N, \\ f\left(\frac{r_c}{t_i}\right) &= \left(\frac{r_c}{t_j}\right)^e \bmod \lambda(N). \end{aligned} \quad (17)$$

Next, the CAS sends the public keys $f(r_c/t_j)$ to every user U_j .

Phase 2: Broadcasting phase. When a user U_1 wants to broadcast a message M to a group of users $GU_1 = \{U_2, U_3, \dots, U_a\}$, the following steps have to be performed.

Step 1: U_1 sends a request message to the CAS indicating the identities of receivers in group GU_1 .

Step 2: The CAS computes B_1 and $f(B_1)$ as follows

$$\begin{aligned} B_1 &= t_1 t_2 \dots t_a \bmod N, \\ f(B_1) &= B_1^e \bmod \lambda(N), \end{aligned} \quad (18)$$

and broadcasts $f(B_1)$ to U_1, U_2, \dots, U_a .

Step 3: U_1 computes the enciphering key MK_1

$$\begin{aligned} MK_1 &= K_1^{f(B_1)^d \cdot f(r_c/t_1)^d} \bmod N \\ &= K_0^{t_1 t_2 \dots t_a r_c} \bmod N \\ &= K_0^{B_1 r_c} \bmod N. \end{aligned} \quad (19)$$

and enciphers message M as $C = E_{MK_1}(M)$.

Phase 3: Decryption phase. Every user U_i , for $2 \leq i \leq a$, computes the key MK_1 from his private key K_i , his public key $f(t_j)$, and the public parameter $f(B_1)$:

$$\begin{aligned} MK_1 &= K_j^{f(B_1)^d \cdot f(r_c/t_j)^d} \bmod N \\ &= K_0^{t_1 t_2 \dots t_a r_c} \bmod N \\ &= K_0^{B_1 r_c} \bmod N. \end{aligned} \quad (20)$$

Next, when a legal user U_j , $2 \leq j \leq a$, receives C , the message M is deciphered.

6. SECURITY AND PERFORMANCE ANALYSIS

The modification proposed in section 5 overcomes the conspiracy attack presented in [1] and the attacks presented in section 4.

Conspiracy attack of two legal users (see [1]). This attack, successfully applied to Liaw's original broadcasting cryptosystem, considers that two legal users U_x , U_y share their private keys t_x , t_y . Since t_x , t_y are relatively prime, two numbers s , r can be obtained satisfying $rt_x + st_y = 1$ by the Euclidean algorithm. Hence, the system key K_0 can be recovered from

$$K_x^r K_y^s \bmod N = K_0^{rt_x} K_0^{st_y} \bmod N = K_0^{rt_x + st_y} \bmod N = K_0 \bmod N. \quad (21)$$

Clearly, this attack cannot be applied to the modified cryptosystem proposed in section 5 since the users do not know parameter t_j . This is the same argument exposed by Tseng and Jan in [1] to avoid the attack.

Factorization of $f(t_j)$. According to [1], in order to obtain t_j , a user should solve the equation $f(t_j) = t_j^e \bmod \lambda(N)$, where only $f(t_j)$ is known, which is not computationally feasible. By the same reason, it is computationally infeasible to get the private key e of CAS from the previous equation, thus preventing the attacks explained in section 3 and [7] for obtaining K_0 .

Recovering system key K_0 . Another way to try recovering K_0 comes from the situation in which a legal user attacks its private key $K_j = K_0^{t_1} \bmod N$. This attack is computationally infeasible as K_0 and t_1 are not known by the user. It is also infeasible to obtain K_0 by

raising K_j to the exponent $f(r_c/t_j)^d$, that is,

$$K_j^{f(r_c/t_j)^d} \bmod N = K_0^{t_j(r_c/t_j)^{ed}} \bmod N = K_0^{r_c} \bmod N, \quad (22)$$

where K_0 and r_c are not known.

Attacks in section 4. The key MK_i now depends on the sender and all the legitimate receivers. Hence, every combination of sender-receivers define a different key. As a consequence, the attacks presented in section 4 have no effect on the modified protocol proposed in this paper.

Performance analysis. The minimum length of $f(t_j)$ is much shorter than the length ($\sim 2^{71}$ bits) suggested in [7] for the Liaw's original cryptosystem to be secure. In our case, the effort to obtain e or t_j is equivalent to factoring $N = pq$, where p, q are safe prime numbers. Hence, the minimum length of $f(t_j)$ is the same as that of N to make infeasible a factorization attack; that is, $2048 = 2^{11}$ bits, approximately [10]. Since all the parameters are integers modulo $\lambda(N)$, the lengths of $f(B_1), f(r_c/t_j), K_j, t_j, e$, and MK_1 are the same: 2^{11} bits. Note that the public RSA exponent d must be short. In this way, the amount of information a user has to keep is 2^{14} bits, corresponding to $f(B_1), f(r_c/t_j), K_j, N, d$, and MK_1 .

The amount of information the CAS has to broadcast is reduced to the length of $f(B_1)$, that is, 2^{11} bits. The same amount of bits is sent to every user in the setup phase.

The decryption phase in section 5 has been designed taking into account the great number of potential users in a real broadcasting network. Because of this, the computational complexity of the algorithm for enciphering/deciphering the key MK_1 does not depend on the number of legitimate receivers. As can be observed from Eq. (19) to (20), only two integer exponentiations (with a short exponent d), two modular exponentiations and one modular multiplication are necessary to compute MK_1 .

7. CONCLUSIONS

We have shown an inconsistency in the improvement of Liaw's cryptosystem proposed in [1]. Moreover, both the improvement and the original scheme [2] suffer several weaknesses which allow illegal users to read enciphered broadcast messages. The modifications proposed in this work overcome the conspiracy attack stated in [1] and the weaknesses shown in the cryptanalysis above. In addition, these modifications reduce the amount of information to be kept and broadcast by the users, thus not suffering the weaknesses pointed out in [7, 8].

REFERENCES

1. Y. M. Tseng and J. K. Jan, "Cryptanalysis of Liaw's broadcasting cryptosystem," *Computers and Mathematics with Applications*, Vol. 41, 2001, pp. 1575-1578.
2. H. T. Liaw, "Broadcasting cryptosystem in computer networks," *Computers and*

- Mathematics with Applications*, Vol. 37, 1999, pp. 85-87.
3. C. C. Chang and T. C. Wu, "Broadcasting cryptosystem in computer networks using interpolating polynomials," *Computer System Science and Engineering*, Vol. 6, 1991, pp. 185-188.
 4. G. H. Chiou and W. T. Chen, "Secure broadcasting using the secure lock," *IEEE Transactions on Software Engineering*, Vol. 15, 1989, pp. 929-934.
 5. W. G. Tzeng and M. S. Hwang, "A conference key distribution scheme for multi-level security," in *Proceedings of 5th National Security Conference*, 1995, pp. 47-52.
 6. H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Maths, Vol. 138, Springer-Verlag, Berlin Heidelberg, 1993.
 7. H. M. Sun, "Security of broadcasting cryptosystem in computer networks," *Electronics Letters*, Vol. 35, 1999, pp. 2108-2109.
 8. M. S. Hwang, C. C. Lee, and T. Y. Chang, "Broadcasting cryptosystem in computer networks using geometric properties of lines," *Journal of Information Science and Engineering*, Vol. 18, 2002, pp. 373-379.
 9. R. Rivest, A. Shamir, and I. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol. 21, 1978, pp. 120-126.
 10. A. J. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," *Journal of Cryptology*, Vol. 14, 2001, pp. 255-293.



Jaime Muñoz Masqué obtained the University degree in Mathematics at the Universidad Central de Barcelona, Spain, in 1973 and the Ph.D. in Science at the Universidad de Salamanca, Spain, in 1983. He was an Assistant Professor from 1979 to 1985 and a full professor from 1985 to 1989, both positions in the Universidad de Salamanca. His research topics are applied mathematics, computer science, information systems, and mathematical physics.



Alberto Peinado Domínguez obtained the Ing. degree in Telecommunications Engineering at the University of Málaga in 1993, and the Ph.D. degree in Computer Science at the Polytechnic University of Madrid, Spain, in 1997. From 1995 to 1998, he was with the National Spanish Council for Scientific Research (CSIC), Madrid, Spain, where his research interests were in cryptography and network security. Since 1998, he has been with the Department of Ingeniería de Comunicaciones at the University of Málaga as an Assistant Professor and then as an Associate Professor. His research interests include cryptography, mobile communications, CDMA codes, smart cards, and watermarking.