Cryptanalysis of Kim et al.'s Traitor Tracing Scheme on ACISP02

Fangguo Zhang and Kwangjo Kim

International Research center for Information Security(IRIS)

Information and Communications Univ.(ICU), Korea

Abstract

At ACISP'02, H.J. Kim *et al.*[1] proposed a new traitor tracing scheme. However, this paper show that the proposed scheme is to be insecure by presenting a conspiracy attack. Using our attack, any two subscribers can collaborate to derive the secret key of the data supplier and tell or sell it to any body. Thus, the unauthorized user can always decrypt the encrypted session key with the decrypted session key. Also the two subscribers cannot be traced by the data supplier.

Key words: Broadcast encryption, Traitor tracing, Conspiracy Attack.

I. Introduction

A traitor tracing scheme, which a provider can use in broadcasting the encrypted digital contents such as pay-TV, is the following: The provider gives a distinct personal key to each authorized user in advance, and broadcasts both the contents encrypted by a session key and the encrypted session key which can be decrypted only by the authorized users; the users decrypt the encrypted session key with their personal keys and recover the contents with the decrypted session key. There are some traitor tracing schemes proposed in [2-4].

Recently, H.J. Kim *et al.* [1] proposed a new traitor tracing scheme that has two-levels for efficiency. The broadcasted encryption messages of this scheme consist of triples of (enabling block, renewal block, cipher block), an enabling block is used only for secure broadcast of a session key and a renewal block is used for detecting and revoking traitors's rights and regenerating the group key. In this paper, we propose an attack on their scheme. In our attack, any two subscribers can collaborate to derive the secret key of the data supplier, and can tell or sell it to any body. So the unauthorized user can always decrypt any transmitted encryption messages. The two collaborated subscribers cannot be traced by the data supplier.

II. Kim et al.'s Traitor Tracing Scheme

First of all, we review Kim *et al.*'s traitor tracing scheme in brief using the same notation as [1].

The data supplier (DS) estimates the number of subscribers in advance and then starts the system setup. Let n be the estimated number of subscribers.

System Setup. Let G be a pseudo random number generator and H be a hash function. DS setups the system as follows:

S1 Choose prime numbers p and q such that $q|p-1$.

S2 Choose a random value $g \in Z_p$ with order q.

S3 Choose randomly $h \in Z_q^*$.

S4 Perform the following steps for $1 \leq i \leq n$.

- Generate the ith random number v_i using the pseudo random number generator G on a random seed value s_v.

- Obtain an output a_{i1} from H based on modulus q on input value v_i. In this time, a_{i1} must contain in Z^*_q. Otherwise, go to S1.

- Compute $a_{i2} \equiv h - a_{i1}$.

If $a_{i2} \notin Z^*_q$, go to S1.

S5 Compute $A_1 \equiv a_{11}a_{21} \cdots a_{n1}a_{r1} (\bmod q)$ and $A_1 \equiv a_{12}a_{22} \cdots a_{n2}a_{r2} (\bmod q)$ with values $a_{r1}, a_{r2} \in_R Z^*_q$.

S6 Select a degree $z(\geq k-1)$ polynomial $f(x) = \sum_{l=0}^{z} a_l x^l$ with $a_l \in Z^*_q$.

S7 Select random values $K_1, K_2 \in_R Z^*_q$ as the group key $x = (K_1^{-1}, K_2^{-1})$.

DS saves the values (h, A_1, A_2), a seed s_v and the polynomial $f(x)$ in secret, and publishes (g, g^h, p, q) and the key set $\langle g^{a_0}, g^{f(1)}, \cdots, g^{f(z)} \rangle$. Finally DS publishes $g^{x_{DS}}$ with $x_{DS} \in_R Z^*_q$ for the self-enforcement property.

Registration. When a new subscriber S_i wants to obtain the authorization of digital contents, DS generates a personal key using values (h, A_1, A_2), a seed s_v and (G, H), and a renewal key using the polynomial $f(x)$. First DS identifies S_i and then sends the keys to him.

- Generate (a_{i1}, a_{i2}) using the value h, s_v, G, and H.

- Compute $\sigma_{i1} = (A_1 / a_{i1})$ and $\sigma_{i2} = (A_2 / a_{i2})$, *i.e.*,

$$\sigma_{i1} = a_{11}a_{21} \cdots a_{(i-1)1}a_{(i+1)1} \cdots a_{n1}a_{r1}$$

$$\sigma_{i2} = a_{12}a_{22} \cdots a_{(i-1)2}a_{(i+1)2} \cdots a_{n2}a_{r2}$$

- Compute $f(i)$.

- Send the pair of personal key $(\sigma_{i1}^{-1}, \sigma_{i2}^{-1})$, the pair of renewal key $(i, f(i))$ and the group key x to S_i.

Encryption of Enabling Block. Let s be a session key such that $s \in Z_p$. An enabling block E is constructed as follows: Let $r, w \in_R Z$ be one-time random numbers.

$$E = \langle s \cdot g^{rh}, g^r, g^{rw^{-1}}, A_1K_1w, A_2K_2w \rangle.$$

DS broadcasts a cipher block and an enabling block containing an encryption message of the session key. The digital contents in a cipher block is encrypted by the session key of a symmetric cryptosystem.

Decryption of Enabling Block. When each subscriber S_i receives a broadcast encryption message, S_i obtains a session key s from the enabling block with his personal key $(\sigma_{i1}^{-1}, \sigma_{i2}^{-1})$ and the group key x as follows:

$$s = s \cdot g^{rh} / g^{rw^{-1}(A_1K_1w \cdot (\sigma_{i1}K_1)^{-1} + A_2K_2w \cdot (\sigma_{i2}K_2)^{-1})}$$

To get digital contents, subscribers decrypt a cipher block using the session key s.

About the renewal phase, the traitor tracing phase and the self-enforcement property of this scheme, the readers can refer to [1] in detail.

III Attack on Kim *et al.*'s Traitor Tracing Scheme

In this section, we give a conspiracy attack on Kim *et al.*'s traitor tracing scheme. In our attack, any two subscribers can recover the secret key of DS and tell or sell any body, *e.g.*, Alice. Then Alice can get the session key s from E using $s \cdot g^{rh}/(g^r)^h$. So she can decode the encrypted contents with the session key. But DS can't trace two subscribers.

We describe the attack in detail as follows: Any subscriber can obtain a relation between A_1 and A_2 from E and the group key x:

$$A_1K_1w \cdot K_1^{-1} / A_2K_2w \cdot K_2^{-1} = \lambda (\bmod q)$$

i.e.,

$$A_1 = \lambda A_2. \quad (1)$$

For any two subscribers, suppose S_i and S_j, they have personal key $(\sigma_{i1}^{-1}, \sigma_{i2}^{-1})$

$(\sigma_{j1}^{-1}, \sigma_{j2}^{-1})$ respectively. Since $\sigma_{i1} = (A_1/a_{i1})$, $\sigma_{i2} = (A_2/a_{i2})$ and $a_{i2} \equiv h - a_{i1}$, we have:

$$A_1 \cdot \sigma_{i1}^{-1} + A_2 \cdot \sigma_{i2}^{-1} = A_1 \cdot \sigma_{j1}^{-1} + A_2 \sigma_{j2}^{-1} \quad (2)$$

From Eqs. (1) and (2), S_i and S_j can solve A_1 and A_2, hence h.

From this fact, we can state that Kim *et al.*'s traitor tracing scheme is vulnerable to the conspiracy attack. Any two subscribers can get the secret key of DS and notify h to any body, then this body can get the session key s from E only using h in the phase of decrypting enabling block.

IV Conclusion

Traitor tracing schemes play an important role in the typical piracy scenario whereby pirate decoders are manufactured and sold by pirates to illegal subscribers. In this letter, we found two linear relationships between the secret keys A_1 and A_2, of the data supplier and proposed a conspiracy attack on Kim *et al.*'s traitor tracing scheme. We had shown that any two subscribers could collaborate to derive the secret key of the data supplier.

References

[1]. H.J. Kim, D.H. Lee and M. Yung, "Privacy against Piracy: Protecting Two-Level Revocable P-K Traitor Tracing", L. Batten and J. Seberry (Eds.): ACISP 2002, LNCS 2384, pp. 482-496, Springer-Verlag, 2002.

[2]. B. Chor, A. Fiat and M. Naor, "Tracing Traitors", In Proc. Advances in Cryptology-Crypto'94, LNCS 839, pp. 257-270, Springer Verlag, 1994.

[3]. K. Kurosawa and Y. Desmedt, "Optimum Traitor Tracing and Asymmetric Schemes", In Proc. Advances in Cryptology-Eurocrypt 98, LNCS 1403, pp. 145-157, Springer Verlag, 1998.

[4]. W. Tzeng and Z.J. Tzeng, "A Public-Key Traitor Tracing Scheme with Revocation using DynamicShares", PKC 01, LNCS 1992, pp. 207-224, Springer Verlag, 2001.