An Improved Traitors Tracing Scheme Based on ELGamal

Ya-Li Qi

The Computer Department, Beijing Institute of Graphic Communication, Beijing, 102600, China

Abstract

The flaw of traitor tracing schemes based on traditional ELGamal is that cannot resist convex combination attack. On this point this paper raises an improved ELGamal scheme, which shorten the length of the private key. The new scheme uses the users private key and the header \( h(s, r) \) to computer session keys. It is worth mentioning that the user’s private key has relation with the header \( h(s, r) \), so the improved scheme has good revocability. The results show that the security of the improved scheme is enhanced in comparison with the traditional traitor tracing scheme.

Keywords: ELGamal, traitor tracing scheme, convex combination attack;

1. Introduction

The goal of a traitor tracing scheme is to provide a method which makes the data suppliers to recover the identity of the traitors with a pirate decoder, \([1,2,3,4,5,6,7,8,9,10,11]\).

ELGamal algorithm has been raised in 1985[2], the security of which is based on the computation difficulty of discrete logarithm over finite domain. For its cryptographic properties it applies to data encryption, digital signature, etc. A recognized flaw of ELGamal encryption scheme is that the ciphertext length is two times of plaintext length. So the traitor tracing scheme usually use two level encryption to improve the efficiency of the broadcast system.

For the traditional ELGamal traitor tracing scheme cannot resist the convex combination attack, many researchers study on it. In \([3,4]\), by increasing the degree of \( f \) from \( k \) to \( 2k-1 \), \( k \)-inclusion resistance can be achieved.

* Corresponding author. Tel.: 13683639502;
  E-mail address: qyl@bigc.edu.cn.
This paper raises a new method based on ELGamal encryption algorithm. Data Supplier (DS) send the users with private key and the header h(s, r) to computer session keys. The private key and the header h(s, r) has close relation based on ELGamal. So the improvement has good revocation because DS can find the traitor from private decoder directly.

In Section 2, we describe the traditional ElGamal traitor tracing scheme and its flaws. Our construction scheme is described in Section 3. We analyze the performance of our scheme in Section 4. Finally, conclusions are given in Section 5.

2. The ElGamal Traitor Tracing Scheme

The ElGamal traitor tracing scheme is two level encryption which can improve the efficiency of the broadcast system. That is to say, information use symmetric encryption and is broadcasted to users. At the same time DS use the encryption algorithm in traitor tracing scheme to produce a data header which send to users too. For users, firstly use the key which is produced by traitor tracing scheme to get to get decryption key, then use the decryption key to decrypt information.

Let p be a prime power, q be a prime such that q|p-1, q>n, (where n is the number of users) and g be a qth root of unity over GF(p).

A Initialization

DS chooses a random polynomial \( f(x) = a_0 + a_1 x + \cdots + a_k x \) over \( \mathbb{Z}_q \) and computes \( y_0 = g^{a_0}, \ y_1 = g^{a_1}, \ldots, \ y_k = g^{a_k} \). Then let \( e_T = (p, g, y_0, y_1, \ldots, y_k) \) be a public key. DS gives \( f(i) \) to authorized user \( u_i \) as personal decryption key \( e_i \), \( 1 \leq i \leq n \).

B Distributing a Session Key

For a session key \( s \), DS computes a header as \( h(s, r) = (g^r, sy_0^r, y_1^r, \ldots, y_k^r) \) where \( r \) is a random number. Then DS broadcasts \( h(s, r) \). Each user \( u_i \) computes \( s \) from \( h(s, r) \) and \( e_i \) as follows:

\[
\left( sy_0^r \times \left( y_1^r \right)^s \times \cdots \times \left( y_k^r \right)^{s} \right)^{f(i)} = s \left( g^r \right)^{f(i)} \left( g^r \right)^{f(i)} = s
\]

C Broadcasting Encrypted Data

To send actual plaintext data \( M \), DS broadcasts \( C = E_s(M) \), where \( E \) is a symmetric key encryption function. Every authorized user can recover \( s \), and then decrypts \( C \) to obtain \( M \).

D Detection of Traitor

When a pirate decoder is confiscated, the pirate key \( e_p \) is exposed. If \( e_p \) contains \( (j, f(j)) \), then DS decides that user \( u_j \) is a traitor.

E Convex attack

Let \( f(1), f(2), \ldots, f(k) \) be \( k \) personal decryption key, \( w = [u, w_0, w_1, \ldots, w_k] \) be any convex combination of the vectors \( v_1, v_2, \ldots, v_k \), defined by:

\[
v_1 = [f(1), 1, i_1, i_1^2, i_1^3, \ldots, i_1^k] \\
\vdots \\
v_k = [f(k), 1, i_k, i_k^2, i_k^3, \ldots, i_k^k]
\]

If there is \( \sum_{i=1}^{k} a_i = 1 \), then we get a vector \( w = \sum_{i=1}^{k} a_i v_i \). The \( w \) is not a legitimate personal decryption key, but it can be used to decrypt any ciphertext like \( C = [a, b_0, b_1, \ldots, b_k] \).
since \( b_0^{w_0} \times b_1^{w_1} \cdots b_k^{w_k} / a^u = s \).

3. The improved scheme

The improvement scheme is two levels encryption too. This paper improves the \( h(r, s) \). The algorithm describes as follow:

A Initialization

DS computes \( \beta = g^x \mod p \), \( x \) is random number as a secret. Then let \( e_T = (p, g, \beta) \) be a public key. DS gives authorized user \( u_i \) as personal decryption key with \( e_i \), \( 1 \leq i \leq n \).

B Distributing a Session Key

For a session key \( x \), DS computes a header as \( h(s, r) \) where \( r \) is a random number. The two parameters meet the conditions as follows:

\[
\beta \equiv g^x \mod p
\]

\[
e_i = x\gamma + rs \mod (p - 1)
\]

Then \( s = (e_i - x\gamma)r^{-1} \mod (p - 1) \)

Because \( \beta \) is public key produced by \( X \), and \( \gamma \) is produced by \( R \). Now takes \( \gamma \) as public key, \( X \) as random number and \( R \) as private key. Then (5) becomes to:

\[
s = (e_i - r\beta)x^{-1} \mod (p - 1)
\]

Then DS broadcasts \( h(s, r) \). Each user \( u_i \) computes \( x \) from \( h(s, r) \) and \( e_i \) as follows:

\[
x = (e_i - r\beta)s^{-1} \mod (p - 1)
\]

C Broadcasting Encrypted Data

To send actual plaintext data \( M \), DS broadcasts \( C = Ex(M) \), where \( E \) is a symmetric key encryption function. Every authorized user can recover \( s \), and then decrypts \( C \) to obtain \( M \).

D Detection of Traitor

When a pirate decoder is confiscated, the pirate key \( e_p \) is exposed. The DS can compare exiting \( s \) and \( r \) with formula

\[
e_i = x\gamma + rs \mod (p - 1)
\]

then DS decides that user \( u_j \) is a traitor.

4. Performance analysis

From the description of the tradition scheme based on ELGamal and the improvement scheme, the important distinguish is length of the private key. The private keys in improvement scheme are based on the ELGamal encryption algorithm. DS sends user \( i \) with \( e_i \) and \( h(s, r) \) as private key of user \( i \).

In fact \( e_i \) has relation with \( h(s, r) \). So the DS sends different user with different private key \( e \), and header \( h(s, r) \). Because every user’ keys are based on random number \( r \), to get session key \( x \) in improvement scheme every user uses his \( e_i \) and \( h(s, r) \) only. Then if the communication is security, the probability of combination attack gets lower. The improvement scheme can resist convex combination attack.
Another advantage of improvement scheme is revocability. It is the revocability that the improved scheme requires the n headers for n users. Although the scheme is based on the public key system, the \( h(r,s) \) for every users has directly relation with his private key \( e_i \). So every user has different private key. Once a private decoder has been confiscated, from the \( e_i \) we can location the user we can cancel his right to use the information. Of cause it based on there is a credible DS.

5. Conclusion

In this paper, we raise an improvement scheme based on ELGamal traitor tracing. By the construct relation between \( e_i \) and \( h(s,r) \), every user use his only private key to get session key \( x \).

The improvement scheme can resistant the convex combination attack which can attack the tradition scheme based ELGamal successfully. And it has good revocability. But there is flaw still. Because the random \( r \) is very important in producing \( h(s,r) \), so the attack to random number \( r \) will affect the security. In order to solve this problem we can increase complexity of random and private key. It is the future research topic.

Acknowledgements

The research is supported by The Foucs Project of Beijing Institute of Graphic Communication Ea2011005 and Funding Project for Academic Human Resources Development in Institutions of Higher Learning Under the Jurisdiction of Beijing Municipality PXM2010_014223_095557.

References


