Chang-Wu 廣播密碼系統之改進

Improvement of the Chang-Wu Broadcasting Cryptosystem Using Interpolating Polynomials

吳宗杉
Wu Tzong-Sun

吳宗成
Wu Tzong-Chen

國立台灣科技大學資訊管理系
Department of Information Management
National Taiwan University of Science and Technology
tcwu@cs.ntust.edu.tw

摘要

1991 年，Chang 與 Wu 利用內插多項式及幾何特性，提出一個廣播密碼系統。1996 年，Hwang 等人和 Lin 與 Chen 分別聲稱 Chang-Wu 的廣播密碼系統不安全。在他們的攻擊中指出，合法的廣播接收者可以推導出發起者或是其他合法接收者的秘密資訊。在本文中，我們將使用單向函數及時戳來改進 Chang-Wu 方法的缺失。在與 Chang-Wu 方法比較之下，我們的改進方法需要更少的公開參數，而且能達到更高之安全強度。

關鍵字：廣播密碼系統、內插多項式、單向函數、時戳。

Abstract

In 1991, Chang and Wu proposed a broadcasting cryptosystem using interpolating polynomials and geometric properties. Hwang et al. (1996) and Lin and Chen (1996) separately claimed that the Chang-Wu broadcasting cryptosystem is insecure. They showed that a malicious user who is a legal receiver of a broadcasting transaction can derive the secrets for the originator and the other legal receivers by plotting another legal broadcasting transaction to these users. With the use of one-way function and timestamp, we propose an improvement of the Chang-Wu scheme. Our improvement can withstand the attacks stated above. As compared to the Chang-Wu scheme, our improvement requires smaller amount of public parameters, while achieving more security strength.

Keywords: broadcasting cryptosystem, interpolating polynomials, one-way function, timestamp.

1. Introduction

A broadcasting cryptosystem is used to achieve secure communications over an insecure channel so that only the specified subset of users can obtain the message in one single broadcasting transaction. In 1991, Chang and Wu [1] proposed a broadcasting cryptosystem using interpolating polynomials and geometric properties. Recently, Hwang *et al.* [2] and Lin and Chen [3] separately demonstrated a successful attack on the Chang-Wu cryptosystem. They showed that in the Chang-Wu scheme, any malicious user who is a legal receiver of a broadcasting transaction can derive the originator's and the other legal receivers' secrets by plotting another legal broadcasting transaction to these users.

With the use of one-way function and timestamp, we shall propose an improvement of the Chang-Wu scheme, and show that our improvement can withstand the attacks stated above. As compared to the Chang-Wu scheme, our improvement requires smaller amount of public parameters, while achieving more security strength. In the next section, we first give a brief review of the Chang-Wu scheme. The attacks on the Chang-Wu scheme are discussed in Section 3. Our improvement and its cryptanalysis are stated in Section 4. Finally, we make conclusions in Section 5.

2. Brief review of the Chang-Wu scheme

The following symbols are used throughout the paper to facilitate the presentation:

CAS:	central authority server;
U_i:	user in the system;
S_i:	the secret point for U_i;
C_i:	the circle i with respect to U_i;
P_i:	the center of C_i;
p_{ij}:	a point on C_i;
$H(x)$:	an interpolating polynomial;
O_i:	a point on $H(x)$;
EP:	Euclidean plane;
$d(x, y)$:	the distance between two points x and y in EP;

The Chang-Wu scheme is described in the following. Suppose that there are $(n + 1)$ users U_0, U_1,

..., U_n in the system. Initially, *CAS* randomly chooses $(n + 1)$ distinct secret points S_i's from *EP*, and distributes S_i to U_i (for $i = 0, 1, ..., n$) via secure channels. One secure broadcasting transaction is divided into two stages: the broadcasting stage (performed by the originator and *CAS*) and the recovery stage (performed by each legal receiver). Details of these two stages are described as below.

The Broadcasting Stage -- Without loss of generality, let U_0 be the originator of the secure broadcasting transaction. First of all, U_0 requests *CAS* that he wants to broadcast a secret message M to U_1, U_2, ..., and U_m $(1 \leq m \leq n)$. Upon receiving U_0's request, *CAS* performs the following tasks:

1. Randomly choose $(m + 1)$ distinct points P_i's (for $i = 0, 1, ..., m$) from *EP*, which are also distinct from S_0, S_1, ..., S_m.
2. Construct an m-degree interpolating polynomial $H(x)$ passing P_0, P_1, ..., P_m.
3. Randomly choose m distinct points O_i's (for $i = 1, 2, ..., m$) from $H(x)$, which are also distinct from P_0, P_1, ..., P_m.
4. Generate $(m + 1)$ circles C_i's (for $i = 0, 1, ..., m$), where each C_i is with P_i as the center and $d(P_i, S_i)$ as the radius.
5. Randomly choose two distinct points p_{i1} and p_{i2} from C_i (for $i = 0, 1, ..., m$), which are also distinct from S_i.
6. Publish O_i's, p_{j1}'s and p_{j2}'s for $i = 1, 2, ..., m$ and $j = 0, 1, ..., m$.

After that, U_0 can originate a secure broadcasting transaction by subsequently performing the following tasks:

7. Calculate C_0 passing S_0, p_{01} and p_{02}, and obtain its center P_0.
8. Reconstruct $H(x)$ with P_0, O_1, ..., O_m.
9. Randomly choose an integer r and compute $k = H(r)$.
10. Broadcast r and the ciphertext of M encrypted by k.

The graphical result of the above procedure is shown as Figure 1.

The Recovery Stage -- Upon receiving r and the ciphertext of M broadcasted by U_0, any legal receiver U_i performs the following steps to recover M:

1. Calculate C_i passing S_i, p_{i1} and p_{i2}, and obtain its center P_i.
2. Reconstruct $H(x)$ with P_i, O_1, ..., O_m.
3. Compute $k = H(r)$ and use it to decrypt the ciphertext.

3. Attacks on the Chang-Wu scheme

The attacks on the Chang-Wu scheme demonstrated in [2, 3] are based on the same idea in essence. From the cryptanalyses discussed in [2, 3], any participants of a broadcasting transaction (including the originator and the legal receivers) can obtain the circles with respect to the others. Such vulnerability makes the Chang-Wu scheme flawed. For instance, U_0 can easily obtain C_2 with respect to U_2 by first finding a line L_2 passing the midpoint of p_{21} and p_{22} satisfying $L_2 \perp \overline{p_{21}p_{22}}$ and then calculating the intersection of L_2 and $H(x)$, i.e., P_2.

Suppose U_0 is the malicious user that wants to derive U_i's secret point S_i (for $i = 1, 2, ..., m$). The scenario of this attack is described as follows. First of all, U_0 originates three broadcasting transactions to the same U_i's. Let C_i, $C_i^{'}$ and $C_i^{''}$ be the circles with respect to U_i for these three broadcasting transactions, respectively. With knowing the fact that C_i, $C_i^{'}$ and $C_i^{''}$ pass S_i, U_0 can easily obtain S_i by finding the intersection of C_i, $C_i^{'}$ and $C_i^{''}$. The graphical illustration of finding the secret point S_i for U_i is shown in Figure 2.

4. Our improvement

In this section, we will present an improvement of the Chang-Wu scheme that can withstand the attacks demonstrated in the previous section. Initially, *CAS* publishes a one-way function f which accepts variable length of input and outputs a point with x- and y-coordinates in Euclidean plane. This one-way function can be easily built by the methods proposed in [4, 5].

The Broadcasting Stage -- First of all, U_0 requests *CAS* that he wants to broadcast a secret message M to U_1, U_2, ..., and U_m $(1 \leq m \leq n)$ at time T. Upon receiving U_0's request, *CAS* performs the following tasks:

1. Randomly choose an m-degree interpolating polynomial $H(x)$.
2. For $i = 0, 1, ..., m$, do the following tasks:
   (2-1). Randomly choose a point Q_i from $H(x)$ and compute P_i satisfying that Q_i is the midpoint of P_i and $f(T, S_i)$.
   (2-2). Repeat from Step (2-1) if there exists some j $(m+1 \leq j \leq n)$ such that $H(x)$ passes the midpoint of P_i and $f(T, S_j)$.
3. Randomly choose m distinct points O_i's (for $i = 1, 2, ..., m$) from $H(x)$, which are also distinct from Q_0, Q_1, ..., Q_m.
4. Publish T, O_i's and P_j's for $i = 1, 2, ..., m$ and $j = 0, 1, ..., m$.

After that, U_0 can originate a secure broadcasting transaction by subsequently performing the following tasks:

5. Calculate the midpoint of P_0 and $f(T, S_0)$, i.e., Q_0.
6. Reconstruct $H(x)$ with Q_0, O_1, ..., O_m.
7. Randomly choose an integer r and compute $k = H(r)$.

8. Broadcast r and the ciphertext of M encrypted by k.

The graphical result of the above procedure is shown as Figure 3.

The Recovery Stage -- Upon receiving r and the ciphertext broadcasted by U_0, any legal receiver U_i performs the following steps to recover the message:

1. Calculate the midpoint of P_i and $f(T, S_i)$, i.e., Q_i.
2. Reconstruct $H(x)$ with Q_i, O_1, ..., O_m.
3. Compute $k = H(r)$ and use it to decrypt the ciphertext.

It is obvious to see that in our improvement, the originator and the legal receivers reconstruct the same $H(x)$. The security of our improvement is based on the capability against the following attacks:

Attack 1. An illegal receiver try to obtain the encryption key k from public information.
Attack 2. Any user in the system try to obtain the other one's secret point from the public information.

Analysis of Attack 1: Since $H(x)$ is an m-degree polynomial, anyone with only knowing m public points O_1, O_2, ..., O_m cannot reconstruct $H(x)$. With the knowledge of S_i, U_i can only find an extra point Q_i, which is the midpoint of P_i and $f(T, S_i)$, unless he is the legal participant (the originator or the legal receiver) for that broadcasting transaction. As to the illegal participant U_j for the broadcasting transaction, he can act like a legal receiver trying to find an extra point on $H(x)$ by finding the midpoint of P_i and $f(T, S_j)$ (for $i = 1, 2, ..., m$) to reconstruct $H(x)$. However, such attack is precluded by Step 2 of the broadcasting stage.

Analysis of Attack 2: Since the secret point S_i for each legal participant U_i for each broadcasting transaction is protected by the one-way function f, anyone cannot obtain S_i from the public information. Moreover, $f(T, S_i)$'s are different for different time T. Even if the attacker has collected historical public information, he still cannot impersonate any one of the legal participants to originate a valid broadcasting transaction.

From the analysis of Attack 2, an attacker cannot succeed in obtaining the secret point for any legal participant in the broadcasting transaction by plotting the same trick demonstrated in [2, 3].

5. Conclusions

With the use of one-way function and timestamp, we have presented an improvement of the Chang-Wu scheme that can withstand the attacks demonstrated in [2, 3]. Our improvement achieves more security strength as compared to the original Chang-Wu scheme. Besides, the amount of public information (T, O_i's and P_j's) required in our improvement is $2m + 2$, whereas the amount of public information (O_i's, p_{j1}'s and p_{j2}'s) in the Chang-Wu scheme is $3m + 2$.

References

[1] Chang, C.C. and Wu T.C., "Broadcasting cryptosystem in computer networks using interpolating polynomials", *Computer Systems Science & Engineering*, Vol. 6, No. 3, 1991, pp. 185-188.

[2] Hwang T., Lee, N.Y., Li, C.H., and Chang, C.C., "On the security of Chang and Wu's broadcasting cryptosystem for computer networks", *Computer Systems Science & Engineering*, Vol. 11, No. 5, 1996, pp. 311-314.

[3] Lin, J.F. and Chen, S.J., "Comment on broadcasting cryptosystem in computer networks using interpolating polynomials", *Computer Systems Science & Engineering*, Vol. 11, No. 5, 1996, pp. 315-317.

[4] Merkle, R. C., "One way hash function and DES", *Advances in Cryptology - CRYPTO '90*, Springer-Verlag, Berlin, 1990, pp. 428-446.

[5] Rivest, R. L., "The MD5 message digest algorithm" RFC 1321, April 1992.

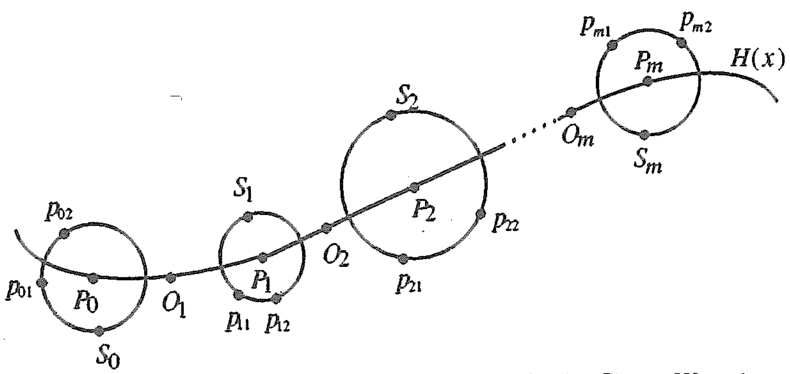

Figure 1. Graphical result of the broadcasting stage in the Chang-Wu scheme.

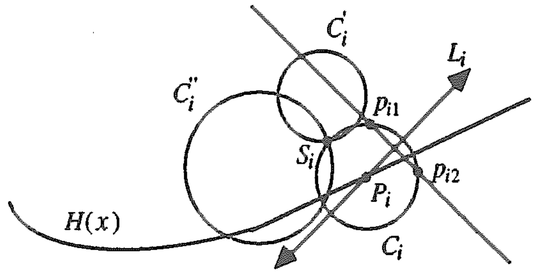

Figure 2. Attack on finding the secret point S_i for U_i.

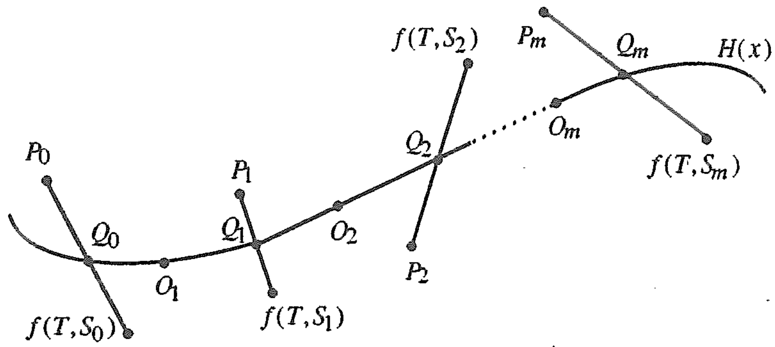

Figure 3. Graphical result of the broadcasting stage in our improvement.