# Broadcasting Cryptosystem in Computer Networks Using Geometric Properties of Lines*


Min-Shiang Hwang† Cheng-Chi Lee‡ Ting-Yi Chang§

Department of Information Management†
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413 , R.O.C.
Email: mshwang@cyut.edu.tw
Fax: 886-4-23742337

Department of Computer and Information Science‡
National Chiao-Tung University
1001 Ta Hsueh Road,
Hsinchu, Taiwan, R.O.C.

Department of Computer Science and Information Engineering§
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413 , R.O.C.


January 19, 2002


*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-004.

# Broadcasting Cryptosystem in Computer Networks Using Geometric Properties of Lines

**Abstract**

In 1997, Wu and Wu proposed an improvement of Chang-Wu broadcasting cryptosystem using geometric properties of lines. The Wu-Wu scheme gave a better performance and required fewer public parameters than the Chang-Wu scheme. In this paper, the authors shall propose an improvement of the Wu-Wu scheme using geometric properties of line. This improvement further reduces the amount of computing time and significantly decreases the parameters required as compared to the Wu-Wu scheme.

*Keywords:* Broadcasting, cryptosystem, security.

## 1 Introduction

In 1989, Laih et al. [4] proposed a new threshold scheme which is based on the definition of cross-product in an N-dimension vector space. Their scheme can be applied for designing conference key distribute systems. The conference key can be used to be an enciphering/deciphering key in the broadcasting cryptosystem.

In 1991, Chang and Wu proposed a broadcasting cryptosystem using interpolating polynomials and geometric properties of circles [1]. Later, in 1997, Wu and Wu proposed an improvement using geometric properties of line to give a better performance and requiring fewer public parameters than the Chang-Wu scheme [12].

In 1999, Liaw [5] proposed a new broadcasting cryptosystem based on the RSA public key scheme [2, 6] and a conventional cryptosystem such as DES

[7]. Liaw claimed that his scheme would require fewer broadcasting messages and it would be easier to insert new users into the system than all previous methods [1, 3, 11]. However, Sun pointed out [9] Liaw's scheme required a very large amount of information for each broadcast and the information had to be kept by each user. Subsequently, Tseng and Jan proposed a conspiracy attack to Liaw's scheme and proposed an improvement [10]. Nevertheless, the improvement had a weakness which Sun pointed out [9].

The Laih et al.'s scheme [4] is different from the Wu-Wu scheme [12]. In [4], there is no central authority server ($CAS$) which is used to distribute the individual secret key to each participant for constructing the conference key. Whoever wants to broadcast a secret message, the originator must have a responsibility to distribute the individual secret key over a secure channel in broadcasting stages. On the other hand, the $CAS$ of the Wu-Wu scheme only need to distribute the secret key over a secure key to each participant one time. The originator only publishes a value to broadcast a secret message. The two schemes have different applications in the broadcasting cryptosystem.

In this article, we shall propose an improvement of the Wu-Wu scheme using geometric properties of line. Our improvement further reduces computing time and requires fewer parameters as compared to the Wu-Wu scheme. Furthermore, it still maintains the advantage of the Wu-Wu scheme.

The remainder of our paper is organized as follows. In Section 2, we briefly review the Wu-Wu broadcasting cryptosystem. In Section 3, we propose an improvement of the Wu-Wu scheme. In Section 4, we analyze the security of our improvement. In Section 5, we compare the performance of our improved scheme with the Wu-Wu scheme. Finally, we give a brief conclusion.

## 2 Review of the Wu-Wu Scheme

In this section, we briefly review the Wu-Wu scheme. The system parameters are defined as follows. $CAS$ denotes the central authority server; $U_i$ denotes a user in the system; $S_i$ denotes the secret distinct point for $U_i$; $P_i$ denotes the distinct point; $Q_i$ denotes the midpoint; $f$ denotes a one-way function published by $CAS$; $T$ denotes a time-variant parameter; $E_k(\cdot)$ denotes the encryption and decryption functions of a symmetric cryptosystem using the session key $k$. $EP$ denotes the Euclidean plane. The scheme is divided into three stages as follows.

**Initiative stage:**

Assume that $(n+1)$ users are in the system. $CAS$ randomly chooses $(n+1)$ $S_i$ from $EP$ and distributes $S_i$ to $U_i$ (for $i = 0, 1, \cdots, n$) via secure channels and then publishes a one-way function $f$. For each secure broadcast, the broadcasting stage is performed by the originator and $CAS$, the recovery stage is performed by each legal receiver as described below.

**Broadcasting stage:**

Assume that $U_0$ is the originator who wants to broadcast a secret message $M$ to $U_1$, $U_2$, $\cdots$, and $U_m$ ($1 \leq m \leq n$). After receiving $U_0$'s request, $CAS$ performs the following tasks:

1. Randomly select a line $L(x)$ from $EP$.

2. Randomly select $(m+1)$ distinct points $Q_i$ from $L(x)$, and computes $P_i$ such that $Q_i$ is the midpoint of $Pi$ and $f(T, S_i)$, for $i = 0, 1, \cdots, m$, where $T$ is a time-variant parameter.

3. Randomly select a point $A$ from $L(x)$, which is distinct from $Q_0, Q_1, \cdots, Q_m$.

4. Publish $T$, $A$ and $P_i$ for $i = 0, 1, \cdots, m$.

After that, $U_0$ can initiate a secure broadcasting transaction by performing the following tasks:

1. Calculate the midpoint of $P_0$ and $f(T, S_0)$, denoted as $Q_0$.
2. Reconstruct $L(x)$ with $Q_0$ and $A$.
3. Randomly select an integer $r$ and compute $k = L(r)$.
4. Broadcast $r$ and the ciphertext $C = E_k(M)$.

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

**Recovery stage:**
After receiving $r$ and $C$, any legal receiver $U_i$ has capability to recover $M$ by performing the following steps:

1. Calculate the midpoint of $P_i$ and $f(T, S_i)$, denoted as $Q_i$.
2. Reconstruct $L(x)$ with $Q_i$ and $A$.
3. Compute $k = L(r)$ and decrypt the message $M$ form $D_k(C)$.

Note that without the knowledge of $S_i$, no one can calculate $f(T, S_i)$. $S_i$ is only known to legal users $U_i$ and $CAS$.

# 3 Our Scheme

In this section, we propose an improvement of the Wu-Wu scheme. The improvement can decrease computing time and still maintain the advantage of the Wu-Wu scheme as described in later sections. The improvement consists of three stages: (1) *initiative stage*, (2) *broadcasting stage*, and (3) *recovery stage*. The *system parameters* $(CAS, U_i, S_i, f, T, E_k(\cdot), EP)$ and the *initiative stage* are the same as that of the Wu-Wu scheme. The details of our improvement are as follows:

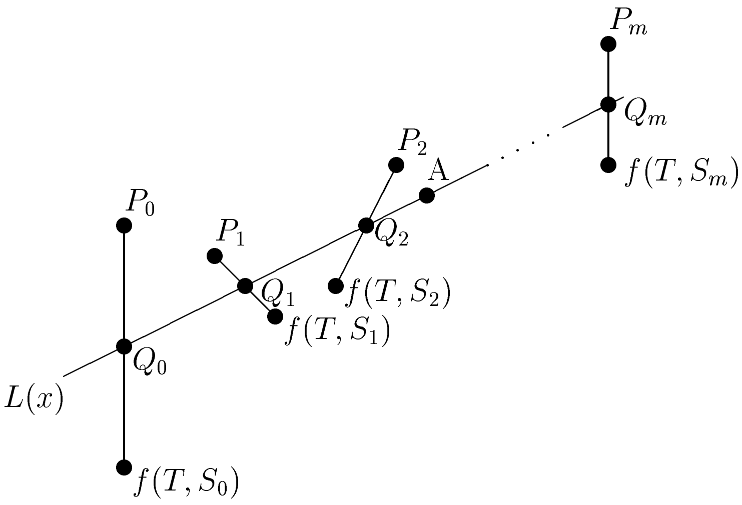


Figure 1: Graphical result of broadcasting stage in the Wu-Wu scheme

**Broadcasting stage:**

Assume that $U_0$ is the originator who wants to broadcast a secret message $M$ to $U_1$, $U_2$, $\cdots$, and $U_m$ ($1 \leq m \leq n$). After receiving $U_0$'s request, $CAS$ performs the following tasks:

1. Randomly chooses a line $L(x)$ from $EP$.

2. Compute $L(f(T, S_i))$ to derive $y_i$, and $(f(T, S_i), y_i)$ is a point on $L(x)$, for $i = 0, 1, \cdots, m$, where $T$ is a time-variant parameter.

3. Randomly choose a point $A$ from $L(x)$, which is distinct from $(f(T, S_i), y_i)$, for $i = 0, 1, \cdots, m$.

4. Publish $T$, $A$ and $y_0$, $y_1$, $\cdots$, $y_m$.

After that, $U_0$ can initiate a secure broadcasting transaction by performing the following tasks:

1. Reconstruct $L(x)$ with $A$ and $(f(T, S_0), y_0)$.

2. Randomly select an integer $r$ and compute $k = L(r)$.

3. Broadcast $r$ and the ciphertext $C = E_k(M)$.

The graphical result of the above procedure is shown in Figure 2.

**Recovery stage:**

After receiving $r$ and $C$, any legal receiver $U_i$ will have the capability to recover $M$ by performing the following steps:

1. Reconstruct $L(x)$ with $A$ and $(f(T, S_i), y_i)$.

2. Compute $k = L(r)$ and decrypt the message $M$ form $D_k(C)$.

Note that without the knowledge of $S_i$, no one can calculate $f(T, S_i)$. $S_i$ is only known to legal users $U_i$ and $CAS$.

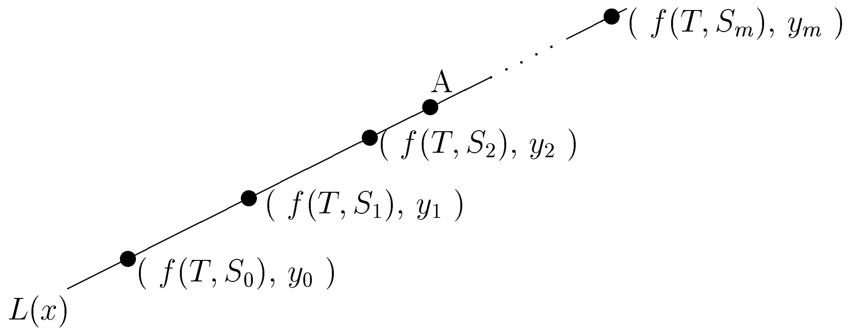


Figure 2: Graphical result of broadcasting stage in our scheme

# 4 Security Analysis

In order to obtain the broadcasting secret message, an adversary or illegal receiver must reconstruct $L(x)$, generated by $CAS$, then compute the session key $k = L(r)$ to decrypt the message $M$. If an adversary or illegal receiver wants to reconstruct $L(x)$, he/she must find two points on $L(x)$. The adversary would then only know of one public point $A$, to find another point on $L(x)$ would be extremely difficult.

An illegal receiver $U_j$ might act as a legal one and compute the point $(f(T, S_j), y_i)$ for reconstructing $L(x)$, we see that the probability of finding the point located on $L(x)$ is equivalent to that of performing an exhaustive search on $k$ [12]. Furthermore, $y_i$ is computed by $L(f(T, S_i))$ and lines $L(x)$ that are time-variant, the adversary or illegal receiver would not be able to accurately determine the extra point that is on current $L(x)$.

# 5 Performance and Storage Analysis

The Wu-Wu scheme used geometric properties of line to give a better performance and required fewer public parameters than the Chang-Wu scheme. In this section, we analyze the performance and storage complexities of our scheme, and compare it with the Wu-Wu scheme.

To analyze the computational complexity of the Wu-Wu scheme and our scheme, we first define related notations as follows. $T_f$: the time for executing the adopted one-way function $f$; $T_L$: the time for constructing a line $L(x)$ giving two distinct points in $EP$; $T_Q$: the time for obtaining the midpoint of two points; $T_{L(r)}$: the time for calculating $L(r)$, where $L(x)$ is a line.

| | Broadcasting stage | Recovery stage |
|---|---|---|
| Wu-Wu scheme | $T_L + (m+2)(T_Q + T_f)+$ $(m+3)T_{L(r)}$ | $T_f + T_Q + T_L + T_{L(r)}$ |
| Our improvement | $T_L + (m+2)T_f + (m+3)T_{L(r)}$ | $T_f + T_L + T_{L(r)}$ |

Table 1: Performance of the Wu-Wu scheme and our scheme

From Table 1, it is obvious that our scheme is more efficient than the Wu-Wu scheme. Our scheme is less $(m+2)T_Q$ and $T_Q$ than the Wu-Wu scheme in the broadcasting stage and recovery stage, respectively. Furthermore, our scheme doesn't need the $Q_i$ points which increases by the number of the participants in the system. Thus, our scheme requires fewer parameters and reduces the computing time.

# 6 Discussions and Conclusions

In order to avoid an adversary pretends to be $U_0$, a legal originator, to host a broadcasting system, both Wu-Wu and our schemes need a secure channel between $U_0$ and $CAS$ to authenticate each other.

Our scheme is a special case of Shamir's secret sharing scheme [8]. Our scheme can be constructed by applying Shamir's $(2, n)$ secret sharing scheme. In our scheme, $CAS$ publishes a point $A$ from $L(x)$. Each participant can use $A$ and $(f(r, S_i), y_i)$ to reconstruct $L(x)$ and obtain the session key $k$.

In this article, we have proposed an improved scheme which modifies some aspects of the Wu-Wu scheme. Our scheme has successfully reduced the computing time and significantly lessened the parameters required. Though modifications were made the original advantages are maintained and un-compromised. In addition, the overall performance and requirements of fewer parameters make our proposed scheme an improvement on the Wu-Wu scheme.

# References


[1] C. C. Chang and T. C. Wu, "Broadcasting cryptosystem in computerusing networks using interpolating polynomials," *Computer System Science and Engineering*, vol. 6, no. 3, pp. 185–188, 1991.

[2] Chin-Chen Chang and Min-Shiang Hwang, "Parallel computation of the generating keys for RSA cryptosystems," *IEE Electronics Letters*, vol. 32, no. 15, pp. 1365–1366, 1996.

[3] G. H. Chiou and W. T. Chen, "Secure broadcasting using the secure lock," *IEEE Transactions aon Software Engineering*, vol. 15, no. 8, pp. 929–934, 1989.

[4] C. S. Laih, L. Harn, and J. Y. Lee, "A new threshold scheme and its applications on designing the conference key distribution cryptosystem," *Information Processing Letters*, vol. 32, no. 3, pp. 95–99, 1989.

[5] Horng-Twu Liaw, "Broadcasting cryptosystem in computer networks," *Computers and Mathematics with Application*, vol. 15, no. 8, pp. 85–87, 1999.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[7] Bruce Schneier, *Applied Cryptography, 2nd Edition.* New York: John Wiley & Sons, 1996.

[8] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.

[9] Hung-Min Sun, "Security of broadcasting cryptosystem in computer networks," *Electronics Letters*, vol. 35, no. 24, pp. 2108–2109, 1999.

[10] Yuh-Min Tseng and Jinn-Ke Jan, "Cryptoanalysis of Liaw's broadcasting cryptosystem," *Computers and Mathematics with Application*, vol. 41, no. 12, pp. 85–87, 2001.

[11] W. G. Tzeng and M. S. Hwang, "A conference key distribution scheme for multilevel security," in *Proceedings of the Fifth National Conference Security*, pp. 47–52, Taiwan, May 2001.

[12] Tzong-Sun Wu and Tzong-Chen Wu, "Improvement of chang-wu broadcasting cryptosystem using geometric properties of lines," *Electronics Letters*, vol. 33, no. 23, pp. 1940–1941, 1997.