JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 18, 373-379 (2002)

Short Paper

Broadcasting Cryptosystem in Computer Networks Using Geometric Properties of Lines*

MIN-SHIANG HWANG, CHENG-CHI LEE [+] AND TING-YI CHANG[++]
Department of Information Management
Chaoyang University of Technology
Taichung Hsien, 413 Taiwan
[+]*Department of Computer and Information Science*
National Chiao Tung University
Hsinchu, 300 Taiwan
[++]*Department of Information and Communication Engineering*
Chaoyang University of Technology
Taichung Hsien, 413 Taiwan

In 1997, Wu and Wu proposed an improvement of the 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 propose an improvement to the Wu-Wu scheme using geometric properties of line. This improvement reduces the computation and significantly decreases the parameters required as compared to the Wu-Wu scheme.

Keywords: broadcasting, cryptosystem, security, geometric, secret sharing

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 to the design of conference key distribution systems. The conference key can be used as 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 lines to give a better performance and require 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

Received September 6, 2001; revised January 8, 2002; accepted February 19, 2002.
Communicated by Chi Sung Laih.
*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC90-2213-E-324-004.

claimed that his scheme would require fewer broadcast messages and it would be easier to insert new users into the system than previous methods [1, 3, 11]. However, Sun pointed out [9] that Liaw's scheme requires 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 needs 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 broadcasting cryptosystems.

In this article we shall propose an improvement of the Wu-Wu scheme using geometric properties of lines. 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 to 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 $i = 0, 1, \ldots, n$) 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, …, and U_m ($1 \le m \le n$). 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 compute P_i such that Q_i is the midpoint of P_i and $f(T, S_i)$, for $i = 0, 1, \ldots, m$, where T is a time-variant parameter.
3. Randomly select a point A from $L(x)$, which is distinct from $Q_0, Q_1, \ldots, Q_m$.
4. Publish T, A and P_i for $i = 0, 1, \ldots, m$.

After this, 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 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 Fig. 1.

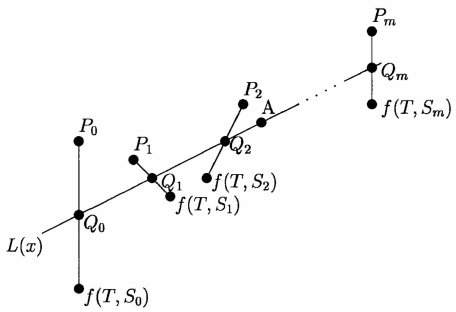

Fig. 1. Graphical result of broadcasting stage in the Wu-Wu scheme.

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 Q_i.
2. Reconstruct $L(x)$ with Q_i and A.
3. Compute $k = L(r)$ and decrypt the message M from $D_k(C)$.

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

3. OUR SCHEME

In this section, we propose an improvement to 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) *ini-*

tiative stage, (2) *broadcast 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 in the Wu-Wu scheme. The details of our improvement are as follows:

Broadcasting stage:

Assume that U_0 is the originator who wants to broadcast a secret message M to U_1, U_2, …, and U_m ($1 \le m \le n$). 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, where $(f(T, S_i), y_i)$ is a point on $L(x)$, for $i = 0, 1, \ldots, m$, and 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 $i = 0, 1, \ldots, m$.
4. Publish T, A and $y_0, y_1, \ldots, y_m$.

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 Fig. 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*.

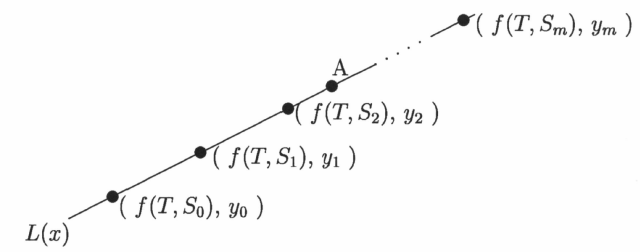

Fig. 2. Graphical result of broadcast stage in our scheme.

4. SECURITY ANALYSIS

In order to obtain the broadcast secret message that was broadcast, an adversary or illegal receiver must reconstruct $L(x)$, generated by *CAS*, and then compute the session key $k = L(r)$ in order to decrypt 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 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 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 uses geometric properties of lines 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 notation. T_f: the time for executing the adopted one-way function f. T_L: the time for constructing a line $L(x)$ given 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.

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

	Broadcast 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 scheme	$T_L + (m + 2) T_f + (m + 3) T_{L_{(r)}}$	$T_f + T_L + T_{L_{(r)}}$

From Table 1, it is obvious that our scheme is more efficient than the Wu-Wu scheme. Our scheme is faster by $(m + 2)T_Q$ and T_Q than the Wu-Wu scheme in the broadcast and recovery stages, respectively. Furthermore, our scheme doesn't need the Q_i points which increases 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 prevent an adversary who pretends to be U_0, a legal originator, from hosting a broadcast 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], in which ours 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 reduced the parameters required. Though modifications were made, the original advantages are maintained and uncompromised. 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, 1991, pp. 185-188.
2. C. C. Chang and M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems," *IEE Electronics Letters*, Vol. 32, 1996, pp. 1365-1366.
3. G. H. Chiou and W. T. Chen, "Secure broadcasting using the secure lock," *IEEE Transactions on Software Engineering*, Vol. 15, 1989, pp. 929-934.
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, 1989, pp. 95-99.
5. H. T. Liaw, "Broadcasting cryptosystem in computer networks," *Computers and Mathematics with Application*, Vol. 15, 1999, pp. 85-87.
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, 1978, pp. 120-126.
7. B. Schneier, *Applied Cryptography*, 2nd ed., New York: John Wiley & Sons, 1996.
8. A. Shamir, "How to share a secret," *Communications of the ACM*, Vol. 22, 1979, pp. 612-613.
9. H. M. Sun, "Security of broadcasting cryptosystem in computer networks," *Electronics Letters*, Vol. 35, 1999, pp. 2108-2109.
10. Y. M. Tseng and J. K. Jan, "Cryptoanalysis of Liaw's broadcasting cryptosystem," *Computers and Mathematics with Application*, Vol. 41, 2001, pp. 85-87.
11. W. G. Tzeng and M. S. Hwang, "A conference key distribution scheme for multilevel security," in *Proceedings of the Fifth National Conference Security*, 2001, pp. 47-52.
12. T. S. Wu and T. C. Wu, "Improvement of Chang-Wu broadcasting cryptosystem using geometric properties of lines," *Electronics Letters*, Vol. 33, 1997, pp. 1940-1941.

Min-Shiang Hwang (黃明祥) received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung Univer-

sity, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field 'Electronic Engineer' in 1988. He also passed the National Telecommunication Special Examination in field 'Information Engineering', qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.

Cheng-Chi Lee (李正吉) received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999 and in 2001. He is currently pursuing his Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, Republic of China. His current research interests include information security, cryptography, and mobile communications.

Ting-Yi Chang (張庭毅) received the B.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999 and in 2001. He is currently pursuing his M.S. in Information and Communication Engineering from CYUT. His current research interests include information security, cryptography, and mobile communications.