A Crypto-broadcast System Based on the New Packet Lock of Factorial Number Representation

Shiuh-Jeng Wang[1], Cheng-Hsing Yang [2]

[1] Department of Information Management Central Police University Taoyuan, Taiwan 333

E-mail: sjwang@sun4.cpu.edu.tw

[2]Department of Information Management Kun-Shan University of Technology

Abstract

In this paper, a new integrated packet technique is proposed to apply to the encrypted message multi-cast in a network link environment. A sum-up packet lock is rather essential in a message's transmission for several different intended recipients in a network system, since the processing time in the message multi-delivery could be substantially reduced. The approaches on the packet integrity employed to the crypto-broadcast system in the past years are either based on the foundation of Chinese remainder theorem or T-base number system. Basically, the later method is somewhat superior to the former used in space requirement of packet construction in the worst case. Following the inspiration of T-base construction, a novel factorial number representation to form the packet lock transmission in a crypto-broadcast system is proposed in this paper. Furthermore, a formal estimation to the magnitude of a constructed packet lock *W(mlogn)* in bit presentation is required, where *m* is the total number of a group of network recipients and *n* is the maximal number among the sub-packets collected from the intended recipients.

Keywords: crypto-broadcast, security, network system, factorial number

I. Introduction

With the rapid development in computer and communication in the most recently year, a secure network message delivery is becoming more and more important. A message transmission in a network basically divided two kinds of point-to-point and point-to-multipoint. The former type is only suitable in a single two-side connection link; it would be quite inefficient on the spending of time and traffic if there a lot of point-to-point links are connected to achieve multi-communication [2]. Therefore, the technical demand of point-to-multipoint has become a very important research issue so as to get a high performance quality of message transmission in a network environment. On the other hand, due to the fact that the message is delivered on the broadcast channels of network system, it is very easy to suffer the intentional threat, such as eavesdropping, interruption, interception, modification and fabrication, and etc. A cryptosystem is thus used to apply to the broadcasting scheme in order to safeguard data against invalid attempt in getting secrecy. Traditionally, a cipher used in the crytosystem can be categorized into secret-key system and public-key system. The secret-key system could get a good speed performance in encryption/decryption manipulation. While there a problem occurs with the system that each user needs to keep a large amount of keys for those communicating partners when the connection links increase dramatically. The concept of public-key was first due to Diffie and Hellman [3]. In the system, each user holds a key-pair, named public key and secret key. The sender can encrypt the message by using the intended receiver's public key and then the receiver is able to decrypt the ciphertext sent from the sender by using his own secret key. In a network system of m users, clearly, there are only *2m* keys required in public-key system, which is very less than the number of keys, total C_2^m, in the secret-key system. There has been received considerable attention from many researchers [1,5,7,10] in crypto-broadcast system. These schemes remained a high security aspect and lower key management with the adoption of public-key system. Among [1,7], the construction of a packet lock summed up from the sub-packets associated with the public keys carries on the one-copy sending of a ciphertext. Follow up the principle of packet lock construction, a new construction technique is proposed in this paper together with public-key system and secret-key system in terms of high security and fast computing to fulfill the requirements of crypto-broadcast system in [2,11].

The organization of our paper is presented as follows. In Sec. II, a preliminary is first given so as to get familiar with our scheme. A crypto-broadcast system with a single packet lock transmission based on the factorial number representation is then proposed in Sec. III. The security discussion and space comparison are addressed in Sec. IV. Next, the

approximate estimations to the space requirement on packets integrity are followed in Sec. V. Finally, the concluding and remarks are given in Sec. VI.

II. Preliminary

Before going our scheme, let us give some theoretical descriptions on the factorial number representation to easily get familiar with our idea.

Lemma 1: For each positive integer n, the inequality $(n+1)! > \sum_{p=1}^{n} p \cdot p!$ *holds.*

Proof: Intuitively, the formula $\sum_{p=1}^{n} p \cdot p!$ can be express as $\sum_{p=1}^{n}(p+1)! - \sum_{p=1}^{n} p!$ and then *(n+1)!-1* is evaluated so that the inequality of $(n+1)! > \sum_{p=1}^{n} p \cdot p!$ is thus satisfied.

Q.E.D.

Theorem 1: Let $SP_0, SP_1, \ldots, SP_{n-1}$ *be positive integers, where* $SP_i \neq SP_j \neq 0$. *There exists a sum integer Z such that*

$$SP_i = \left\lfloor \frac{Z}{a_i} \right\rfloor \bmod [T-(i-1)], \tag{1}$$

where $T = \max\{SP_0, SP_1, \cdots, SP_{n-1}\}$ *and* $a_i s$ *are product integers corresponding to* SP_i *for* $i = 0,1,2\cdots n,$ *respectively.*

Proof: Let the positive integers, $SP_i s, i = 0,1,\ldots n-1,$ be in decreasing order expression as follows $SP_0 > SP_1 > SP_2 > \ldots > SP_{n-1}$.

Let $T = SP_0$ and define a_i as the rules

$$\begin{cases} a_i = \prod_{j=n-2}^{i} (T-j), & 0 \le i < n-1, \\ a_i = 1, & i = n-1, \end{cases} \tag{2}$$

where the product symobl $\prod_{j}^{i}$ is only executed on the condition of $j \ge i$ with decreasing order. Then the Z can be constructed with the form as $Z = \sum_{i=0}^{n-1} a_i (SP_i)$.

For each SP_i, it could be performed exactly by (1), the reasons are given as follows.

$$\begin{aligned} &\left\lfloor \frac{Z}{a_i} \right\rfloor \bmod [T-(i-1)] \\ &= \left\lfloor \frac{a_0(SP_0) + a_1(SP_1) + \cdots + a_{i-1}(SP_{i-1}) + a_i(SP_i) + a_{i+1}(SP_{i+1}) + \cdots + a_{n-1}(SP_{n-1})}{a_i} \right\rfloor \\ &\bmod [T-(i-1)] \\ &= \lfloor m + SP_i + g \rfloor \bmod [T-(i-1)], \end{aligned} \tag{3}$$

where

$$m = \frac{\sum_{j=0}^{i-1} a_i (SP_j)}{a_i} \tag{4}$$

and

$$g = \frac{\sum_{j=i+1}^{n-1} a_j (SP_j)}{a_i} \tag{5}$$

In μ, the denominator

$$a_i = [T-(n-2)][T-(n-2-1)]\cdots[T-(i+1)][T-i]$$

and the items $a_j s$ of numerator, $j = 0,1,2,\ldots,(i-1)$ are expressed as follows:

$$\begin{cases} a_0 = [T-(n-2)][T-(n-2-1)]\cdots[T-i][T-(i-1)]\cdots[T-1][T], \\ a_1 = [T-(n-2)][T-(n-2-1)]\cdots[T-i][T-(i-1)]\cdots[T-1], \\ \vdots \\ a_{i-1} = [T-(n-2)][T-(n-2-1)]\cdots[T-i][T-(i-1)]. \end{cases}$$

Apparently, it does hold for $a_i \left| \sum_{j=0}^{i-1} a_j (SP_j), \right.$ the (4) has thus the result as

$$m = [T-(i-1)]\cdots[T-1]T(SP_0) + [T-(i-1)]\cdots[T-1](SP_1) + [T-(i-1)](SP_{i-1}). \tag{6}$$

On the other hand, we consider the evaluation of γ in (5) as

$$g = \frac{a_{i+1}(SP_{i+1}) + a_{i+2}(SP_{i+2}) + \cdots + a_{n-2}(SP_{n-2}) + a_{n-1}(SP_{n-1})}{a_i}.$$

Define

$$\begin{aligned} W &= 1 \cdot 2 \cdot 3 \cdots [T-(n-2)-1] \\ &= [T-(n-2)-1]! \end{aligned}$$

and

$$A = a_{i+1}(SP_{i+1}) + a_{i+2}(SP_{i+2}) + \cdots + a_{n-2}(SP_{n-2}) + a_{n-1}(SP_{n-1}),$$

where

$$\begin{cases} a_i = [T-(n-2)][T-(n-2-1)]\cdots[T-(i+2)][T-(i+1)][T-i], \\ a_{i+1} = [T-(n-2)][T-(n-2-1)]\cdots[T-(i+2)][T-(i+1)], \\ a_{i+2} = [T-(n-2)][T-(n-2-1)]\cdots[T-(i+2)], \\ \vdots \\ a_{n-3} = [T-(n-2)][T-(n-2-1)], \\ a_{n-2} = [T-(n-2)], \\ a_{n-1} = 1. \end{cases}$$

The γ is thus represented as $\gamma = \frac{A}{a_i}$.

For the *A*, we multiply *W* to *A* as *A' = W*A* such that

$$\begin{aligned} A' &= W \cdot A \\ &= [T-i-1]!\cdot(SP_{i+1}) + [T-i-2]!\cdot(SP_{i+2}) + \cdots + [T-(n-2)]!\cdot(SP_{n-2}) + \\ &\quad [T-(n-2)-1]!\cdot(SP_{n-1}) \\ &\le [T-i-1]![T-i-1] + [T-i-2]![T-i-2] + \cdots + [T-(n-2)]![T-(n-2)] + \\ &\quad [T-(n-2)-1]![T-(n-2)-1] \\ &< (T-i)! \end{aligned}$$

which is followed the fact of *Lemma 1*. Consequently, $A' < (T-i)!$ is concluded. Besides, due to

$$\begin{aligned} (T-i)! &= 1 \cdot 2 \cdot 3 \cdots [T-(n-2)-1][T-(n-2)] \cdots [T-i] \\ &= W \cdot [T-(n-2)][T-(n-2-1)] \cdots [T-i] \\ &= W \cdot a_i, \end{aligned}$$

it implies $A' < W \cdot a_i$. Then $A < a_i$ is found out so

that the evaluation of γ is less than 1.

Overall the derivation in our process, clearly, we obtain $[T-(i-1)]|m$ in (6) and γ in (5) is in range of (0,1). As a result, SP_i in (3) is correctly extracted. Thus the theorem.

Q.E.D.

Next, let us take a numerical example as follows to illustrate our theorem mentioned above.

Example 1: Assume that there exists a sequence of four elements, $(11,9,12,7)$. In order to pack these numbers into a fixed integer Z, the four elements in decreasing way is first to be done, so that $N_0 = 12$, $N_1 = 11$, $N_2 = 9$, *and* $N_3 = 7$, i.e. the relation of $N_0 > N_1 > N_2 > N_3$ is satisfied. Then let $T = \max\{12,11,9,7\} = 12$. The items a_i associated with $N_i, i = 0,1,2,3$, respectively, is computed by (2) as follows:

$$a_0 = \prod_{j=2}^{0}(T-j)$$
$$= (T-2)(T-1)T$$
$$= 10 \cdot 11 \cdot 12$$
$$= 1320,$$
$$a_1 = \prod_{j=2}^{1}(T-j)$$
$$= (T-2)(T-1)$$
$$= 10 \cdot 11$$
$$= 110,$$
$$a_2 = \prod_{j=2}^{2}(T-j)$$
$$= (T-2)$$
$$= 10,$$

and

$$a_3 = 1.$$

Accordingly, $Z = \sum_{i=0}^{3} a_i N_i = 17147$ is then resulted.

Next, we show how to get each N_i with Z by (1).

$$N_0 = \left\lfloor \frac{Z}{a_0} \right\rfloor \bmod [T-(-1)]$$
$$= \left\lfloor \frac{17147}{1320} \right\rfloor \bmod 13$$
$$= 12 \bmod 13$$
$$= 12,$$
$$N_1 = \left\lfloor \frac{Z}{a_1} \right\rfloor \bmod T$$
$$= \left\lfloor \frac{17147}{110} \right\rfloor \bmod 12$$
$$= 11,$$
$$N_2 = \left\lfloor \frac{17147}{10} \right\rfloor \bmod 11$$
$$= 9,$$

and

$$N_3 = \left\lfloor \frac{17147}{1} \right\rfloor \bmod 10$$
$$= 7,$$

which is clearly the same as the original sequence given in our example.

Based on the proof of previous theorem, There indeed exists an integer constant Z mixing of an integer set of $\{SP_0, SP_1, .., SP_{n-1}\}$such that each integer SP_i could be exactly extracted by (1). Accordingly, the research is inspired.

III. A Crypto-broadcast System Based on the Factorial Number Presentation System

Here there are some indications of symbol to be shown first as follows in order to facilitate the reading of our scheme.

Symbols description:

1. U_i: A recipient of message multi-cast in a network system

2. PKS: A public-key system in which each user holds a key-pair of public key and secret key

3. (USK_i,UPK_i): A key-pair of secret key USK_i and public key UPK_i associated with each U_i defined on the *PKS*

4. $E_{UPKi}(\cdot)/D_{USKi}(\cdot)$: An enciphering/deciphering algorithm with a ciphering key UPK_i/USK_i. The message $(\cdot)$ can be revealed by performing $D_{USKi}(E_{UPKi}(\cdot))= (\cdot)$ on the *PKS*

5. M: A transferred message issued from a network user, named originator

6. K_s: A session key used to encrypt the message *M*, randomly chosen by the originator

Assume that there exists *m+1* user of group *G* in a network system. A network message multi-cast could be launched by anyone, say $U_{originator}$, who is among the members in *G* of the network system. Consider a group of intended recipients containing *k* members, denoted by $SG=\{U_0, U_1, U_2, .., U_{k-1}\} \acute{I} G$. Each message *M* is required to be encrypted in advance against the illegal eavesdropping and interception before broadcasting out. Obviously, this work could be done by using the encryption of $E_{ks}(M)$ with session key K_s. The K_s is needed to be shared with each U_i in *SG* so as to let U_i could exactly catch the original M by executing the decryption of $D_{ks}(E_{ks}(M))$ in the receiving end. How to secretly share K_s among the members in *SG* undoubtedly becomes a keen concern in crypto-broadcast system. Generally, the K_s is first embedded into a sub-pack SP_i formed from the intended recipient U_i, a packet lock *Z* is then constructed by compacting all sub-packets associated with the U_is in *SG*. Finally a one-copy of *Z* conjunction with related public information is broadcasted out simultaneously. Each U_i who extracts the sub-packet SP_i based on Theorem 1 could get the common session key by cracking SP_i

individually. The M is thus revealed. The detailed algorithms to understand our approach are shown as follows:

Algorithm 1: Construction of a single packet lock {The algorithm is performed by a message originator.}
Input: An originator $U_{originator}$ and a set of intended recipients, SG.
Step 1: Generate randomly a session key K_s.
Step 2: Compute the temporary SP_j for each intended recipient U_j in SG by performing $SP_j=E_{UPKj}(K_s)$.
Step 3: Rearrange the SP_j of U_j in decreasing order such that $T=SP_0>SP_1>SP_2>..>SP_{k-1}$, and record the mapping index list IL between the new SP_i and U_j , where $IL= \{(i,j) \mid for\ each\ (SP_i, U_j), i,j=0,1,2,.., k-1\}$.
Step 4: Construct the packet lock Z by applying *Theorem 1* in which the variable n replaces with k.
Step 5: Output K_s, Z, T and IL.
■

Following the Algorithm 1, the originator encrypts the M with K_s as $C=F_{Ks}(M)$, where the F is a cipher algorithm on a secret-key system, such as IDEA, FEAL-N (with N runs). Afterward, the packet lock Z and the related public information of $\{C, T, IL\}$ is sent out in the network system.

Algorithm 2: Recovery of a session key and revelation of a transferred message {The algorithm is performed by each intended recipient in SG when receiving the broadcasted information.}
Input: The Z and $\{C, T, IL\}$
Step 1: Compute the sub-packet SP_j according to Z and the index mapping of (i,j) in IL :

$$SP_j=\left\lfloor \frac{Z}{a_i} \right\rfloor \bmod T-(i-1),$$

where $a_i=\prod_{r=k-2}^{i}(T-r)$, for $0 \pounds r \pounds k-2$ and $a_{k-1}=1$.
Step 2: Decrypt the session key $K_s=D_{USKj}(SP_j)$.
Step 3: Decrypt the original message $M=F^{-1}_{Ks}(C)$, were F^{-1} denotes the deciphering algorithm with the key K_s on a secret-key system.
Step 4: Output the M.
■

IV. Security and Space Analysis

The used cryptographic ciphers in our proposed algorithms would be strongly established under a hybrid system made of the high-security guaranteed public-key system and the fast-computing secret-key system. The security mainly rests part in either the difficulty of solving discrete logarithm, such as DH, ElGamal system [4,5], or the intractable on breaking the factorization on a large composite number, RSA [8] for instance. Basically, the physical threat faced in our scheme is the revelation of session key. Once the session key is exposed, the transferred message would be decrypted and known to those who illegal intruders. The possible attacks imposed on session key might come from two ways including insider people in the same receiving group SG and outsider people, not in SG. Whatever which attack, the illegal intruder at most get the sub-packet by (1) for recipients in SG. It is rather hard to probe the session key embedded the sub-packet even the sub-packet is revealed carelessly because our scheme is assumed on the high-security aspect of public-key system as mentioned above. Therefore, the threat of gaining the session key is released.

Next, we give a simple treatment for the space construction of packet lock in our scheme by comparing that of [7]. Assume that the public-key system adopted in our scheme is also the same as the used system in [7]. Review the lock in [7] represented as $Q=\sum_{i=1}^{m} R_i(p+1)^{i-1}$, where m is the total number of users in the network system, R_i is a sub-packet and p is a large prime. Intuitively, $R_i=SP_j$ would hold if we let the generation of sub-packet SP_j in our scheme be the same as the procedure of generating R_i in their scheme. Evidently, $Z=\sum_{i=0}^{m-1}(SP_i)a_i$ is less than Q for the sake of $T=max\{SP_i \mid i=0,1,2,..,m-1\}<(p+1)$ and $a_i=\prod_{r=m-2}^{i}(T-r) < (p+1)^{m-1-i}$ *for* $i=0,1,.., m-2$ and $a_{m-1}=1$. That is to say, the space size of packet lock indeed has been efficiently reduced in comparison with [7].

V. Space Requirement on Packet Lock Construction in a Crypto-broadcast System

In a crypto-broadcast system, a message is usually encrypted before sending out so as to safeguard the secrecy of the message on a public channel, such as public switching communication network in wire-line case and mobile radio communication in wireless case. As previously mentioned in Sec. I, the public-key system is a good scenario in both reducing key number and maintaining key management so that it is naturally incorporated into most crypto-broadcast systems. Review the packet lock X construction in [1], the X is formed from the Chinese remainder theorem (abbreviated with CRT) as follows:

$$\begin{Bmatrix} R_1 = X \bmod N_1 \\ R_2 = X \bmod N_2 \\ \vdots \\ R_i = X \bmod N_i \\ \vdots \\ R_m = X \bmod N_m \end{Bmatrix},$$

where N_i is relatively prime to N_j, N_i¹N_j. The $X=\sum_{i=1}^{m}(S_i * R_i * b_i) \bmod L$, where $L=\prod_{i=1}^{m} N_i$, $S_i=\prod_{\substack{j=1 \\ j\neq i}}^{m} N_j$ and $b_i * S_i \bmod N_i = 1$. Apparently, the value of X falls in the range of $[0, L-1]$. Let us take the smallest primes $N_1, N_2, .., N_i, .., N_m$ in increasing to product to be the L in order to conveniently analyze the magnitude of X. In [9] the Prime Number Theory tell us, the number of primes that are small than m is approximately m/lnm when m is large, where lnm denotes the natural logarithm of m. In other words, the index i is proportional to $N_i/(ln(N_i))$. Therefore $X=\prod_{i=1}^{m} N_i$ in the worst case is great than $\prod_{i=1}^{m} i * \ln(i+1)$ such that X > $m!(lnm)$. This inequality could be substituted with $m! \approx \sqrt{2\pi m}\,(m/e)^m$ by the Stirling's approximation formula in [6], then $X > \sqrt{2\pi m}\,(m/e)^m(lnm) > (m/e)^m(lnm)$ is leaded. As a result, the X is at least great than the value of $(m/e)^m(lnm)$ such that $W(mlogm)$ in bit representation is required on packet lock construction with CRT.

Instead of CRT, the T-base system is somewhat simple to form in technical aspect as follows. Given a sequence of m integers, $R_1, R_2, .., R_i, .. R_m$, each R_i could be gained as follows:

$$\begin{Bmatrix} R_1 = \left\lfloor \frac{Y}{T^0} \right\rfloor \bmod T \\ R_2 = \left\lfloor \frac{Y}{T^1} \right\rfloor \bmod T \\ \vdots \\ R_i = \left\lfloor \frac{Y}{T^{i-1}} \right\rfloor \bmod T \\ \vdots \\ R_m = \left\lfloor \frac{Y}{T^{m-1}} \right\rfloor \bmod T \end{Bmatrix},$$

where $Y=\sum_{i=1}^{m} R_i T^{i-1}$ is so-called packet lock and $0<R_i<T$ for $i=1, 2, .., m$. In a manner that the magnitude of Y is bounded by $\sum_{i=1}^{m}(T-1)T^{i-1} = T^m-1$. The order $O(T^m)$ with Y in the worst case is thus found out. With the previous discussions that the bit representation for Y is $O(mlogT)$ needed. In contrast with $X=\prod_{i=1}^{m} N_i$ (N_i is relatively prime to N_j and $N_i > R_i$) estimated from CRT, the measured magnitude on the space requirement for the boundary of $Y= T^m-1$ would be less that of X in the worst case when the R_i is over $GF(T)$. In other words, the T-base system is superior to the CRT used on the packet construction in this viewpoint. Next, let us take a look for our construction of Z based on the factorial number representation. In a similar discussion as previous section, the $Z=\sum_{i=0}^{m-1}(SP_i)a_i$, where $0<SP_i<T$, $a_i=\prod_{r=m-2}^{i}(T-r) < T^{m-1-i}$ for $i=0,1,..,m-2$ and $a_{m-1}=1$. Accordingly, the magnitude of Z is clearly less than $Y=\sum_{i=1}^{m} R_i T^{i-1}$ with T-base system. As a matter of fact how large required on the space of packet construction and which technique exploited on compacting the sub-packets are still kept interesting to the crypto researchers in the most recent years. In the following, a theoretical description on space requirement with lower bound to the packet lock is specified. As a result, the measurement on a packet construction should conform to our analysis whatever any possible packing mechanisms are used in a crypto-broadcast system.

Definition 1: D_i be the m different encrypted messages in length of B_i-bit, i=1, 2,.., m, respectively, in a crytpo-broadcast system.

Definition 2: A packing lock PL means that providing a method Y_{PL} to gather together all D_i into a packet lock $Y_{PL}(D_1, D_2, .., D_m)$ in total length of B_G bits.

Definition 3: An unpacking UP means that providing a method Ψ_{UP}^{-1} to gain an exact $D_i = \Psi_{UP}^{-1}(Y_{PL}(D_1, D_2, .., D_m))$.

Theorem 2: B_G is W(mlogn) in the worst case, where $n = max(D_1, D_2, ... D_m)$.

Proof: Suppose that there exists a space Z to represent the magnitude of $Y(D_1, D_2, .., D_m)$ such that D_i can be exactly gained by the manipulation as $\Psi_{UP}^{-1}(Y_{PL}(\cdot))$ and $|Z| < \sum_{i=1}^{m} B_i$, where $|Z|$ denotes the bit-length with Z. Apparently, there are $2^{\sum_{i=1}^{m} B_i}$ possible messages appearance for $(D_1, D_2, \ldots D_m)$. On the other hand, the number of possible occurrences for the message Z are only $2^{|Z|}$ less than $2^{\sum_{i=1}^{m} B_i}$. Upon the principle of pigeonhole, there must be a fact that at least two different messages in

$(D_1, D_2, \ldots D_m)$ fall into the same location corresponding to a message in Z. Obviously, it is a contradiction to the *Definition 3* for an exact D_i revealed. Thus, the length of $|Z| \geq \sum_{i=1}^{m} B_i$ is concluded. Also due to the fact that $|Z| \geq \sum_{i=1}^{m} B_i$, B_G in *Definition 2* is indeed great than $\sum_{i=1}^{m} B_i$. Consider the maximal encrypted message $n = max\ (D_1, D_2, \ldots D_m)$, the bit-length *mélognù* is evaluated for B_G in the worst case so that the bit representation *W(mlogn)* with B_G is required. Thus the theorem.

Q.E.D.

VI. Concluding and Remarks

In this paper, we have proposed a new packet integrity technology in a crypto-broadcast system. The packet lock is constructed from the theoretical foundation of factorial number representation. Meanwhile, the cryptographic technique suggested in our scheme is based on the public-key system, like DH or RSA system. Thereby, our scheme could provide more flexible choices to withstand a variety of attacks in the network system. In general, the features of a crypto-broadcast include:

- One-copy of packet lock is sent out and then received simultaneously by many intended destinations.
- The analysis of information traffic in the broadcast set must be strongly prevented from a cryptanalyst.
- The operation in message encryption and decryption are reqired to be minimized.

Overall our scheme, only one-copy of a single packet lock issued by a message originator is sent out. A public-key system is adopted to prevent the session revelation from intruder's cryptanalysis, such as chosen-plaintext attack, during the broadcast transmission. And the physical message is encrypted/decrypted (with the common session key) under the secret-key system, it has ever been estimated that the execution time is much less than the usage of public-key system, i.e. the recovery of a broadcast message is fast. Overall, the main features in a crypto-broadcast system mentioned above are satisfied in our scheme. Furthermore, we also give a theoretical estimation on the space magnitude of a pack lock construction that *W(mlogn)* in bit representation is required in the worst case. In now the demand of bandwidth is more and more important and the message multi-cast is quite popular in the telecommunication network. Accordingly, we do believe that our scheme could be efficiently implemented in the network broadcast applications, and remain a high flexibility on security consideration.

Acknowledgement:
We are appreciated the anonymous referees' many useful comments to improve the paper's presentation.

References

[1] G. H. Chiou and W. T. Chen, "Secure Broadcasting Using the Secure Lock," IEEE Trans. Software Engineering, Vol. 15, No. 8, 1989, pp. 929-934.

[2] D. E. Denning, Cryptography and Data Security, Addision-Wesley, Reading, Mass., 1982.

[3] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, Vol. 22, No. 6, 1976, pp. 644-654.

[4] T. Elgamal, "A Public Key Cryptosystem and a signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, Vol. 31, No. 4, 1985, pp. 469-472.

[5] I. Ingemarsson, D. T. Tang and C. K. Wang, "A Conference Key Distribution System," IEEE Trans. Information Theory, Vol. 28, No. 5, 1982, pp. 714-720.

[6] D.E. Knuth, The Art of Computer Programming, Vol. 1: Fundamental Algorithms, Second Edition, Addision-Wesley Reading Mass., 1980.

[7] C. H. Lin, C. C. Chang and R. C. T. Lee, "A Conference Key Broadcasting System Using Sealed Locks," Information Systems. Vol. 17, No. 4, 1992, pp. 323-328.

[8] R.L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystem," Communication of ACM, Vol. 21, No. 2, 1978.

[9] K.H. Rosen, "Elementary Number Theroy and Its Applications," Second Edition, Addision-Wesley, Reading, MA, 1988.

[10] H. M. Sun and S. P. Shieh, "Secure Broadcasting in Large Networks," Computer Communications, Vol. 21, 1998, pp. 279-283.

[11] V. L. Voydock and S. T. Kent, "Security Mechanism in High-Level Network Protocols," Computing Surveys, Vol. 15, No. 2, 1983.