International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 24 (2017) pp. 15475-15483

A Key Distribution Scheme in Broadcast Encryption Using Polynomial Interpolation

Deepika M P
Research Scholar, Department of Computer Applications,
Cochin University of Science and Technology, Ernakulum,Kerala, India.
Orcid Id: 0000-0003-0282-5674

Dr. A Sreekumar
Associate Professor, Department of Computer Applications,
Cochin University of Science and Technology, Ernakulum,Kerala, India.

Abstract
Broadcast encryption is a type of encryption scheme first proposed by Amos Fiat and Moni Naor in 1993. Their original goal was to prove that two devices, previously unknown to each other, can agree on a common key for secure communications over a one-way communication path. Broadcast encryption allows for devices that may not have even existed when a group of devices was first grouped together to join into this group and communicate securely. This paper describes broadcast encryption in general, a brief survey on the same, and a new scheme for the key distribution in broadcast encryption using polynomial interpolation. The proposed scheme is a revocation scheme.

Keywords: Broadcast encryption, Data sharing, Revocation scheme, Key Distribution, Polynomial Interpolation.

INTRODUCTION

Traditionally, secure transmission of information has been achieved through the use of public-key cryptography. For this system to work, communicating devices must know about each other and agree on encryption keys before transmission. Broadcast encryption seeks to solve the problem of two devices, previously unknown to each other, agreeing upon a common key. This can allow for new devices, even if they did not exist when the encrypted data was made, to be added to a group of acceptable devices. Since the same data is being sent to all devices, instead of a separately encrypted message for each, broadcast encryption must also ensure that only those devices in the privileged group will be able to decode the mess. A. Fiat and M. Naor [1] first proposed the concept of broadcast encryption in 1993. In this scheme, sender allows to send a cipher text to some designated groups whose members of the group can decrypt it with his or her private key. However, nobody outside the group can decrypt the message. Broadcast encryption is widely used in the present day in many aspects, such as VoIP, TV subscription services over the internet, communication among group members or from someone outside the group to the group members. This type of scheme also can be extended in networks like mobile multi-hop networks, which each node in these networks has limitation in computing and storage resources.

In general, to broadcast (verb) is to cast or throw forth something in all directions at the same time. It is something like as shown in Figure.1

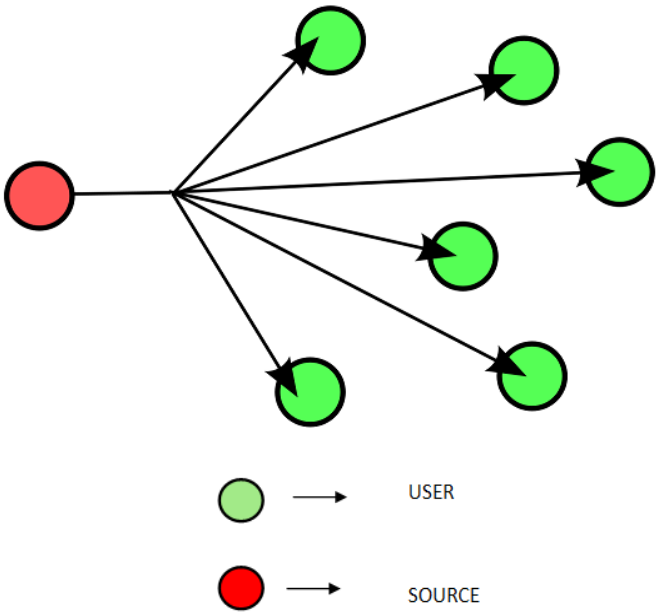

Figure 1: Broadcast Encryption

In practice most Broadcast Encryption systems are smartcard-based. It has been well documented that pirate smartcards (also called pirate “decoders”) are commonly built to allow non-paying customers to recover the content. Broadcast encryption schemes can be coupled with traceability schemes to offer some protection against piracy. If a scheme has x-traceability, then it is possible to identify at least one of the smartcards used to construct a given pirate card provided at most x cards are used in total. When a pirate card is discovered, the keys it contains are necessarily compromised and this must be taken into account when encrypting content. Earlier work in traceability does not deal with this; instead,

the analysis stops with the tracing of smartcards (or, traitor users).

RELATED WORKS

Broadcast encryption is the cryptographic problem of delivering encrypted content (e.g. TV programs or data on DVDs) over a broadcast channel in such a way that only qualified users (e.g. subscribers who have paid their fees or DVD players conforming to a specification) can decrypt the content[1][2][4] . Several papers considered the problem of a center who wants to broadcast to a group [3][5][7][9][10].However, all these schemes are "one-time", and the keys must be updated after every use. The main challenge arises from the requirement that the set of qualified users can change in each broadcast emission, and therefore revocation of individual users or user groups should be possible using broadcast transmissions, only, and without affecting any remaining users. So as efficient revocation is the primary objective of broadcast encryption, solutions are also referred to as revocation schemes [3][7].

Amos Fiat; Moni Naor [1] introduced broadcast encryption scheme in 1994.Broadcast encryption (BE) is a cryptographic method for a centre to efficiently broadcast digital contents to a large set of users so that only non revoked users can decrypt the contents. They considered a scenario where there is a center and a set of users. The center provides the users with prearranged keys when they join the system. At some point thecenter wishes to broadcast a message (e.g. a key to decipher a video clip) to a dynamically changing privileged subset of the users in such a way that non-members of the privileged class cannot learn the message. There are two solutions for this. One is give every user its own key and transmit an individually encrypted message to every member of the privileged class. This requires a very long transmission (the number of members in the class times the length of the message). Another simple solution is to provide every possible subset of users with a key, i.e. give every user the keys corresponding to the subsets it belongs to. This requires every user to store a huge number of keys. Amos Fiat; Moni Naor [1] provided solutions which are efficient in both measures, i.e. transmission length and storage at the user's end.

In [1] broadcast encryption centre distributes to each user u the set K_u of keys called the user key set of u in the setup stage. We assume that the user keys are not updated afterwards, that is user keys are stateless. A session is a time interval during which only one encrypted message is broadcasted. The session key SK is the key used to decrypt the contents of the session. In order to broadcast a message M, the centre encrypts M using the session key SK and broadcasts the encrypted message together with a header which contains encryption of SK and the information for non revoked users to recover SK. In other words the centre broadcasts:

$< Header;\ \ E_{SK}(M) >$

Where E_{SK}(M) is a symmetric encryption of M by SK.

Then every non revoked user u computes F(K_u ,header) = SK; and decrypts E_{SK}(M) with SK where F is a predefined algorithm .But for any revoked user u, F(K_u ,header) should not render SK. The length of the header, the computing time of F and the size of a user key are called the transmission overhead. The main issue of broadcast encryption is to minimize the transmission overhead with practical computation cost and storage size.

J.A. Garay, J. Staddon and A. Wool [6] proposed the notion of *long-lived broadcast encryption* schemes, whose point is to adapt to the presence of compromised keys and continue to broadcast securely to privileged sets of users. Their basic approach is as follows. Initially, every user has a smartcard with several decryption keys on it, and keys are shared by users according to a pre defined scheme. When a pirate decoder is discovered, it is analyzed and the keys it contains are identified. Such keys are called "compromised," and are not used henceforth. Similarly, when a user's contract runs out and she is to be excluded, the keys on her smartcard are considered compromised. Over time, we may arrive at a state in which the number of compromised keys on some legitimate user's smartcard rises above the threshold at which secure communication is possible using the broadcast encryption scheme. In order to restore the ability to securely broadcast to such a user, the service provider replaces the user's old smartcard with a new one containing a fresh set of keys. Keys also need to be replaced if the contract for a given device has expired. As mentioned before, although it is not likely because of the large space of device keys, it is possible for all the keys to be compromised and for the encryption scheme to break. Garay, Staddon, and Wool seek to minimize the number of smartcards that will need to be replaced in a given period of time they define as an epoch. At the end of an epoch, the service provider must compute which users need to have smart cards replaced to continue secure communications. Thus, the cost of such a scheme becomes directly related to the cost of periodically replacing a number of smart cards in each epoch. For situations in which pirate decoders provide themselves and other unprivileged users access to content, traitor tracing schemes can be employed. Traitor-tracing schemes aim to make the construction of pirate decoders risky because once a compromised key is found; the smart card it came from can be revoked.

The first practical broadcast encryption scheme was proposed in 2001 by Naor et.al, called *subset Difference* (SD) method. This was improved by Halevi and Shamir in 2002 by adopting the notion of layers and thereby the improved scheme is called the *Layered Subset Difference* (LSD) method [8].Both SD and LSD are based on tree structure. To be more precise, let *N* be the total number of users and r be the number of revoked users. The SD scheme requires *2r* transmission overhead and

O $(log^2 N)$ storage size for each user. The computation cost is only *O(log N*) computations of one way permutations. The LSD scheme reduces the storage size to *O* $(log^{3/2} N)$ while keeping the computation cost same. But the transmission Overhead increases to *4r* in LSD.

Halevy, Dani and Adi Shamir [8] proposed *the layered subset difference (LSD) scheme,* enables each user to store one kilobyte worth of keys on a smart card and the broadcast centre can thereby revoke any number of users out of about 256million users by transmitting at most *4r* messages and on average *2r* messages . The basic idea in all the stateless broadcast encryption schemes is to represent any privileged set as the union of *S* subsets of users of a particular form. A different key is associated with each one of these sets, and a user knows a key if and only if he belongs to the corresponding set. The broadcaster encrypts the program key *S*times under all the keys associated with the sets in the cover. Consequently, each privileged user can easily access the program, but even a coalition of all the non-privileged users cannot find the program key. The simplest implementation of this idea is to cover the privileged set with singleton sets. A better solution is to associate the users with the leaves of a binary tree, and to cover the privileged set of leaves with a collection of sub trees. However, these covering strategies are inefficient when the privileged set is the complement of a small number of revoked users.

The LSD method is based on creating the set of privileged users by performing inclusion and exclusion operations on subsets of users. Each subset has a key associated with it. Again, this can be most easily accomplished by grouping users in a balanced binary tree, with each vertex representing a key that all leaf nodes in that sub tree know, and then including or excluding certain sub trees. This nesting inclusion and exclusion of subsets allows the following scenario. Consider a football game being broadcast on a national level to a cable television company's subscribers. The television company allows all subscribers access to the broadcast, except for the local network where a blackout is in place. However, sports bars in the local viewing area with a special subscription are allowed to receive the broadcast, while any sports bar without the special subscription is still excluded. If the subscribers are grouped in a tree structure based on geography and subscription type this operation could easily be performed using the LSD method. If the leaf nodes are not grouped in a logical way, essentially the message will have to be encrypted using mostly leaf node keys and the number of messages broadcast will be on the order of the number of devices. This would be extremely impractical, so the grouping becomes very important.

Yevgeniy Dodis, Nelly Fazio [11] proposed *Public Key Broadcast Encryption for Stateless Receivers.* A revocation scheme within the Subset-Cover framework is fully specified by defining the particular Subset-Cover family S used, the algorithm to find the cover for the authorized set of subscribers and the key assignment employed to deliver to each user the keys corresponding to all the sets the user belongs to. We remark that the key assignment method does not necessarily give each user all the needed keys explicitly, but may provide some succinct representation sufficient to efficiently derive all the needed keys. As specific examples, the Complete Sub tree (CS) method and the Subset Difference (SD) method were formalized and proven secure within the Subset-Cover framework; recently, the Layered Subset Difference (LSD) method was introduced as an improvement on the SD method, that makes it possible to reduce the amount of storage required from each user at the cost of a small increase in the length of each broadcast.

Although all the above methods were proposed for the symmetric setting, in some applications it might be desirable to have revocation schemes within the Subset Cover framework in the public key scenario. To this aim, the authors presented a general technique to transpose any Subset-Cover revocation scheme to the asymmetric setting. The basic idea of this method is to make the public keys associated to each subset in the family *S* available to all the (not necessarily trusted) parties interested in broadcasting information, in the form of a Public Key File (PKF). The price paid for the full generality of this technique is a high in efficiency in term of storage required to maintain and distribute the Public Key File. However, for specific schemes, it might be possible to come up with public key cryptosystems that allows compressing the PKF to a reasonable size. A solution for the more interesting case of the SD method (or equivalently for the LSD scheme) was left as an open problem.

Later, Nam-Su Jho, Hwang [14] proposed *One way chain based broadcast encryption schemes*. It is a new broadcast encryption scheme based on the idea of "one key per each punctured interval". It has been a general belief that at least one key per each revoked user*(r)* should be included in the overhead and hence' *r'* seems to be the lower bound of the transmission overhead in any broadcast encryption scheme with reasonable computation cost and storage size .In our scheme with p-punctured c-intervals ,however the transmission overhead is about :

$$\frac{r}{p+1} + \frac{N-r}{C}$$

Which breaks the barrier of r .This scheme is very flexible with two parameters p and c. If a user device allows a large key storage like set-top boxes and mobile devices then we may take p as large possible to reduce the transmission overhead which is more expensive. If a user device has limited storage and computing power like smart cards and sensors, then we may set c as small as possible. Another remarkable feature of this scheme is that it does not have to preset the total number of users ,any number of additional users can join at anytime ,which is not possible in tree based schemes.

Norranut, Pipat[12] proposed *Broadcast Encryption Based on Braid Groups* cryptography which is an alternative method in the public key cryptography and can reduce the computational cost. The concept of braid groups assists to avoid modular exponential operation in computation cost and the key tree helps in reducing the communication cost to constant round, so the computation cost and the communication cost can be minimized. The asymmetric group key agreement (ASGKA) which was introduced by Wu et al., and the dynamic asymmetric group key agreement (DASGKA) which was introduced by Zhao et al and then propose our broadcast encryption scheme based on braid groups. In Wu et al. scheme, they propose an asymmetric group key agreement protocol based on Aggregatable Signature Based Broadcast (ASBB). An ASGKA protocol has the advantage over a symmetric group key agreement (GKA) protocol in that the ASGKA protocol can verify the sender of a message.

Typically in an ASGKA protocol, it has two keys; one is a public group key, which is used as an encryption key for a message to a group and another is a private key, which a group member can use it individually as a decryption key, but in Wu et al. scheme which is based on ASBB, the encryption process is done by using a public group key and the decryption process is done by using a signature of a sender. This signature can be verified by using the public key of that sender. Their scheme does not require any controllers. As mentioned in Wu et al., their scheme does not improve in communication overhead for one-time group applications in which the members of the group are about fully dynamic as in ad hoc networks, because their scheme has heavy communication overhead in key establishment.

The Zhao et al. [15] scheme is constructed to fulfill the former scheme by introducing a dynamic asymmetric group key agreement. This scheme supports the environment in which users can join or leave the group efficiently without triggering a new key agreement protocol. There are two significant differences between the schemes. The first is that they obtain different decryption key. The decryption key for each member in the former scheme is different but in the later scheme is the same. The second is that the former scheme does not achieve dynamic joining and leaving while the later does. Our scheme is also an ASGKA protocol based on the braid groups based cryptography. We design some protocols which support for the dynamic group broadcast such as join and leave protocols and get better efficiency. The scheme is made up of three algorithms; setup, encryption, and decryption. In the setup phase, when any user needs o join a group, he sends a join request message to a director. The director is one of the group members and everyone knows a public braid denoted as g. Each user can compute their own public keys P_{ki} from their private key k_i and the public braid g. We use the key tree mentioned above to construct a public group key. The public group key $p_k$group can be computed individually from a user private key k_i and other public key according to a position of node in the tree. The concept of braid groups assists to avoid modular exponential operation in computation cost and the key tree helps in reducing the communication cost to constant round, so the computation cost and the communication cost can be minimized.

A.Muthulakshmi, R. Anitha[13] proposed *Identity-based broadcast encryption for multi-privileged groups using CRT* .Most group oriented applications require strict access control mechanisms to prevent unauthorized access to the group communication and hence protect the data. Access control is normally achieved by encrypting the group communication using a secret key shared by the privileged users of the group. Broadcast encryption is an information fusion technique constructing an encrypted broadcast message by exploiting unique information of the users belonging to the receiver set. However, key management becomes an issue when new users join or existing users quit. The concept of identity-based cryptography introduced by Shamir[16] overcomes the above mentioned the selected users' identities. This scheme is constructed using Chinese remainder theorem (CRT) and it achieves constant size cipher text when a message is broadcast to different users in a multi-privileged group. Identity-based broadcast encryption is tool for communicating multiple copies of a single message to a selective group of users, identified by their identities in such a manner that others are unable to access the content. A multi-privileged group is a group of users where the users have different access privileges. This proposes an identity-based broadcast encryption scheme for multi-privileged groups that preserves the identities of the users which is developed using Chinese remainder theorem and bilinear pairing. It also ensures forward and backward secrecy with reference to user join and leave. Security of the scheme is proven under random oracle model.

CRT is an ancient but important calculation algorithm in modular arithmetic. The CRT enables to solve simultaneous equations with respect to different moduli in considerable generality. The concept of secure broadcasting on broadcast channels using CRT was discussed by Chiou and Chen [4] (1989). The authors had constructed a secure lock of the session using CRT in such a manner that only intended recipients can recover the key for decrypting the broadcast content. A secure verifiable secret sharing scheme based on CRT, with periodically renewed user shares, without changing the long-term secret scheme was presented by Kaya and Selçuk (2010)[17]. An identity-based broadcast encryption scheme for multi-privileged groups that preserves the user's privacy using CRT and bilinear pairing is proposed in this paper. The system preserves both forward and backward secrecy and the privacy of the users. Also it provides an easy way for revocation of users, and provides stateless broadcast. The users have to provide O (1) size memory for private key storage. The receiver needs to compute only one pairing which is lesser as compared to the existing schemes and the proposed scheme does not demand any exponent computation from receiver end. Another advantage of this scheme is the

size of the cipher text is not linear in the number of users, but it is linear in the number of service groups.

The proposed method

A new scheme for the key distribution in broadcast encryption using polynomial interpolation is proposed. The proposed scheme is not one time scheme, i.e. no need to update the key after every use. The scheme is based on the Lagrange Polynomial Interpolation. In this section first we will see an introduction to the Lagrange Polynomial Interpolation and there after the key distribution in the case of broadcast encryption using Lagrange Polynomial Interpolation is addressed.

Note on Lagrange polynomial interpolation:

The Lagrange interpolating polynomial is the polynomial$P(x)$ of degree$\leq (n-1)$ that passes through the (n) points $\big(x_1, y_1 = y_1 = f(x_1)\big)$, $\big(x_2, y_2 = y_2 = f(x_2)\big)$, ..., $\big(x_n, y_n = y_n = f(x_n)\big)$, and is given by

$$P(x) = \sum_{j=1}^{n} P_j(x)$$

Where

$$P_j(x) = y_j \prod_{k=1}^{n} \frac{x - x_k}{x_j - x_k} \quad where\ k \neq j$$

Written explicitly,

$$P_x = \frac{(x-x_2)(x-x_3)\ldots.(x-x_n)}{(x_1-x_2)(x_1-x_3)\ldots.(x_1-x_n)} y_1 + \frac{(x-x_1)(x-x_3)\ldots.(x-x_n)}{(x_2-x_1)(x_2-x_3)\ldots.(x_2-x_n)} y_2 + \cdots + \frac{(x-x_1)(x-x_2)\ldots.(x-x_{n-1})}{(x_n-x_1)(x_n-x_2)\ldots.(x_n-x_{n-1})} y_n$$

The formula was first published by Waring (1779), rediscovered by Euler in 1783, and published by Lagrange in 1795.

For Example

Interpolate $f(x) = x^3$ over the range $1 \leq x \leq 3$.

The points are $(x_0, y_0)=(1,1)$

$(x_1, y_1)=(2,8)$

$(x_2, y_2)=(3,27)$

The interpolating polynomial is;

$$P(x) = 1.\frac{x-2}{1-2}.\frac{x-3}{1-3} + 8.\frac{x-1}{2-1}.\frac{x-3}{2-3}. + 27.\frac{x-1}{3-1}.\frac{x-2}{3-2}$$

$$P(x) = 6x^2-11x+6$$

How to use Lagrange interpolate to share a secret and to reconstruct it from a set of point pairs(x, y)?

Let Secret *D=10* and we consider a 3 share scheme that is all of the three shares are needed to reconstruct the secret. We pick two random numbers as the coefficients. Using the coefficients and the secrets the polynomial is constructed as $5x^2+2x+10$.Where 5 and 2 are the selected coefficients and 10 is the secret. By using the constructed polynomial 3 points are generated ;*(1, 17), (2, 34), (3, 61).*

To reconstruct the secret *D*, we need to take care of the constant part of Lagrange's polynomial.

$$l_0 = \frac{(x-2)}{(1-2)}.\frac{(x-3)}{(1-3)} = \frac{(x-2)(x-3)}{2}$$

$$l_1 = \frac{(x-1)}{(2-1)}.\frac{(x-3)}{(2-3)} = \frac{(x-1)(x-3)}{-1}$$

$$l_2 = \frac{(x-1)}{(3-1)}.\frac{(x-2)}{(3-2)} = \frac{(x-1)(x-2)}{2}$$

We can reconstruct the secret D, by ignoring the x es, considering only the constant parts;

$$D = 17.\frac{(-2)(-3)}{2} + 34.\frac{(-1)(-3)}{-1} + 61.\frac{(-1)(-2)}{2} = 10$$

The same method should work for finite field GF(2^8) as long as the arithmetic are replaced with finite field arithmetic.

The key distribution in broadcast encryption using polynomial interpolation

Here we have considered a scenario where there is a broadcast center (BC) and a set of users. The BC provides the users with prearranged keys when they join the system. Consider the Figure 2. Shows the selected scenario, here we can say U is the set of all users comes under the broadcast centre.

$$U=\{u_1,u_2,u_3\ldots u_n\}$$

Suppose we have some messages that are intended for a group of users say T in U. And those messages should not be visible to other users in U. Figure 3 Shows the present condition. The possible solution is encrypting the messages and broadcast the messages. The proposed method is useful for the key distribution in such scenario.

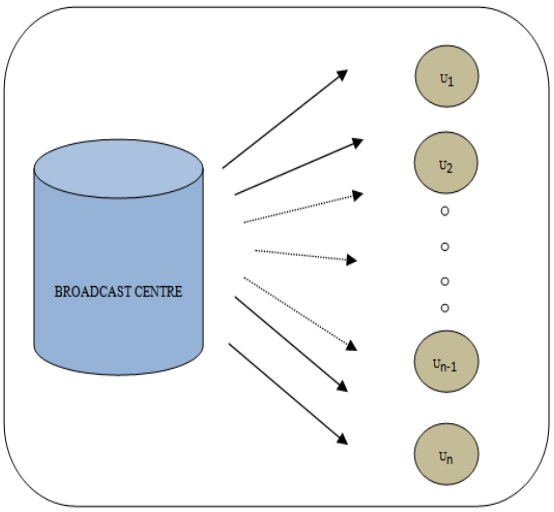

Figure 2: BC with users

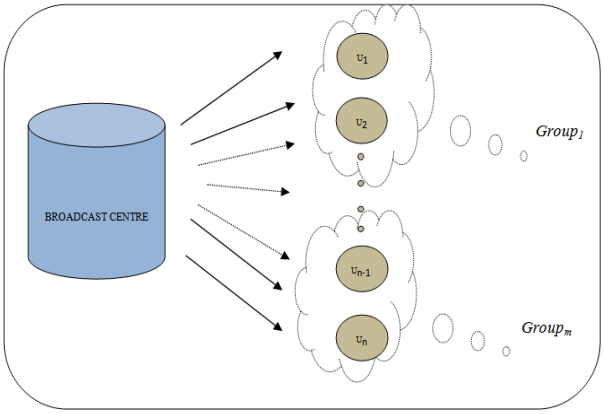

Figure 3: BC with group of users.

Suppose M is the message that is intended for the Group of users T. The Broadcast centre should encrypt the message using a key, say K and send to the users. We can represent the Scenario as follows;

C= E(M,K)

Where M is the message

K is the key

E is the encryption scheme.

C is the encrypted message.

Now at the user's side the decryption should be possible. For decrypting the message, the key K should be available at the user side.

In our proposed method instead of sharing the original key, K, with the users of the group T, we are generation some share of the original key and distribute the shares to the users instead of the original key. And by using the share at the user side we can decrypt the original messages that are intended for the group T. Algorithm. I (a) shows the distribution of the shares of the key among the users in a particular group. Algorithm .I(b) shows the encryption process using the Key. Algorithm.II shows the decryption of each user using the shares of the key.

Suppose *M* is the message that should be distributed securely among the users in the group *T*. The number of users in the group, T is *n* .Initially the broadcast centre has to select a key *K* and a constant *z*.

Algorithm I. (a)

Input:K; the key
Output: $k_1, k_2 \ldots\ldots k_n$; the shares of key

1. START.
2. Select z random numbers as the coefficients say C_1, $C_2, \ldots..C_{z-1}$, C_z of polynomial.
3. Construct polynomial of the form;
$$f(x) = C_1x^z + C_2x^{z-1} + \cdots + C_{z-1}x^2 + C_zx^1 + M$$
4. Select a separate token for each users say, $T_1, T_2, \ldots$ … T_n
5. Find f (T_1), f (T_2)….f (T_n) values save as the shares of the key, Say$k_1, k_2 \ldots\ldots k_n$
6. For each user select a random number say R_i
7. For each user find two more quantities
$k_{iR}= f(T_i+R_i)$
$k_{i2R}= f(T_i+2R_i)$
8. Combine the key factors for each user i
$K_i= (k_i,k_{iR},k_{i2R})$
9. For each user u_i distribute the K_i.
10. STOP.

Algorithm I.(b)

Input: M ; the message
K ; the key
Output : C; the encrypted message for the users of group T.

1. START.
2. Encrypt the message M by using the key K
C= E(M,K)
3. Broadcast the encrypted message C to the group T.
4. STOP.

Assume that the $user_i$ from the Group T is decrypting the message using his own key share.

Algorithm II.

Input: C; the encrypted message
K_i ; the key share of $user_i$
Output: M; the decrypted message.

1. START
2. Accept the random number of the user i, R_i
3. Accept the token of the user T_i
Represent the K_i as 3 pair values. Say (x_1,k_1), (x_2,k_2), (x_3,k_3),
We know $K_i= (k_i,k_{iR},k_{i2R})$
x_1,= T_i ;k_1= k_i,
x_2,= T_i +1*R_i;k_2 = $k_{i(R)}$
x_3=T_i +2*R_i;k_3 = $k_{i(2R)}$
4. Compute the key $K = k_i l_i(x) + k_{i(R)} l_{i(R)}(x) + k_{i(2R)} l_{i(2R)}(x)$
Where
$$l_i(x) = \frac{(x-k_2)}{(x_1-x_2)} \cdot \frac{(x-k_3)}{(x_1-x_3)}$$
$$l_{i(R)}(x) = \frac{(x-k_1)}{(x_2-x_1)} \cdot \frac{(x-k_3)}{(x_2-x_3)}$$
$$l_{i(2R)}(x) = \frac{(x-k_1)}{(x_3-x_1)} \cdot \frac{(x-k_2)}{(x_3-x_2)}$$
6. Perform the decryption using the key K
M = (C, K)
7. STOP

In practical case, the main thing that we have to take care is the parameters with the broadcast centre and each user. It is shown in the Table 1.

Table 1: Parameters with BC

Broadcast Centre:	
M	Number of Groups under that broadcast centre.
User Information	The basic information related to the users.
Information of each group with the Broadcast centre:	
N	Number of users in the group
$T_1T_2T_3...T_N$	The token number of each user in the group
K	The key used for the encryption
Information at each user:	
T_i	The token number of the user*i*
K_i	The key share of the user *i* $K_i = \{k_i, k_{iR}, k_{i2R}\}$ Where R is the random number selected by the user.

Consider an example;

Assumptions: Suppose there are 8 users under a broadcast centre, BC. And there are two groups under the broadcast centre say U and V. Suppose the group U contain the 3 members and V contains 5 members. Let's consider the group U which is having 3 members.

Encryption phase

Before broadcasting, the BC selects the secret key for a group, say K_u.(we are considering the group U).

Suppose the selected K_u is 255.

For constructing the polynomial, the degree of the polynomial (z) and a set of constants as coefficients (C_1, C_2, ... C_{z-1},C_z) of the polynomial are to be selected. Suppose

$z = 3$

$C_1, C_2, C_3 =$ 19,13,83

So the polynomial is,

$$f(x) = C_1x^3 + C_2x^2 + C_3x^1 + K$$

$$f(x) = 19x^3 + 13x^2 + 83x^1 + 255$$

Now select tokens for the users, say T_1T_2 *and* T_3

If T_1= 15 then k_1 is calculated as follows;

$$f(15) = 19 * 15^3 + 13 * 15^2 + 83 * 15^1 + 255$$

k_1 = 68550

Suppose the random number selected for the user is,

R= 2 find f(15+2),f(15+2*2)

$$f(17) = 19 * 17^3 + 13 * 17^2 + 83 * 17^1 + 255$$

= 104770

$$f(19) = 19 * 19^3 + 13 * 19^2 + 83 * 19^1 + 255$$

=136846

Then K_1=(68550, 104770,136846)

IfT_2= 5 then k_2 is calculated as follows;

$$f(5) = 19 * 5^3 + 13 * 5^2 + 83 * 5^1 + 255$$

k_2 = 3370

Suppose the random number selected for the user is,

R= 1 find f(5+1),f(5+2*1)

$$f(6) = 19 * 6^3 + 13 * 6^2 + 83 * 6^1 + 255$$

=5325

$$f(7) = 19 * 7^3 + 13 * 7^2 + 83 * 7^1 + 255$$

=7990

Then K_2=(3370,5325,7990)

IfT_3= 3 then k_3 is calculated as follows;

$$f(3) = 19 * 3^3 + 13 * 3^2 + 83 * 3^1 + 255$$

k_3 = 1134

Suppose the random number selected for the user is,

R= 3 find f(3+3),f(3+2*3)

$$f(6) = 19 * 6^3 + 13 * 6^2 + 83 * 6^1 + 255$$

=5325

$$f(9) = 19 * 9^3 + 13 * 9^2 + 83 * 9^1 + 255$$

=15906

Then K_3=(1134,5325,15906)

Initially the BC selects the tokens for the user and generates the shares of the key for the users in the group. While encryption the message is encrypted by using the Key K. The full process is depicted in Figure 4.

Decryption phase

Consider the user 1(U_1), who belongs to the group K_u.v

During the decryption phase each participant is verified by the corresponding token at the user interfaces itself, then the Key K is reconstructed by using the shares of key which is provided by the participant. As per the algorithm for key reconstruction calculation is as follows;

The user provides his Token (T_1 =15), random number (R_1=2), along with its key share, K_1 = (68550, 104770, 136846).

The K_1 is represented as 3 pairs ;(x_1,k_1), (x_2,k_2), (x_3,k_3)

x_1,= 15 ;k_1= 68550

x_2,= 15 + 1*2= 17;k_2 = 104770

x_3= 15 + 2*2=19;k_3 =136846

Compute

$$K = 68550*\frac{(-104770)}{(15-17)}\frac{(-136840)}{(15-19)} + 104770\frac{(-68550)}{(17-15)}\frac{(-136846)}{(17-19)} + 136846\frac{(-68550)}{(19-15)}\frac{(-104770)}{(19-17)}$$

K=255

Perform the decryption using the key K

M = (C, K)

The complete process is given in the Figure 5.

CONCLUSION

The encryption keys play a vital role in almost all kind of encryption and decryption. Here we addressed a scheme in which the broadcast center doesn't share the key with any of the participating users/subscribers. The shares of the key are distributed instead of the original key. The main advantage is that, the revocation of the user doesn't lead to the requirement of the new key for encrypting the secret and for broadcasting the same.

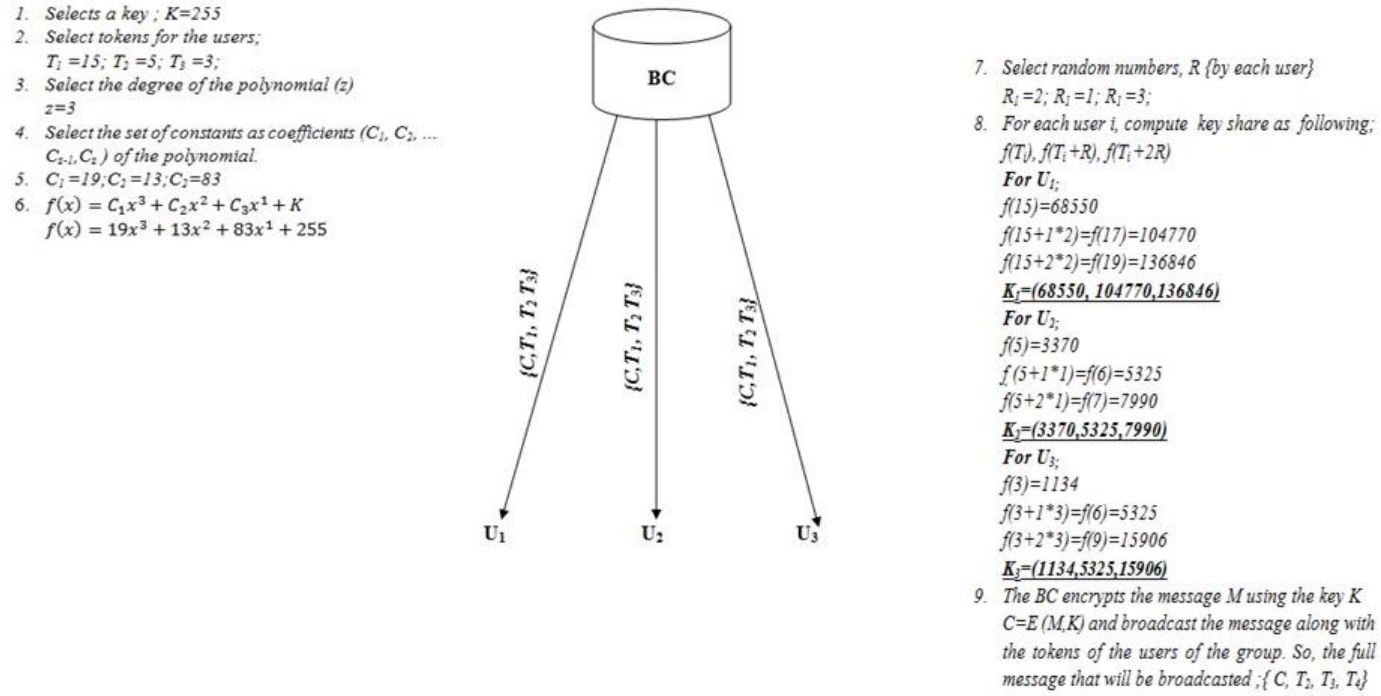

Figure 4: Encryption Phase

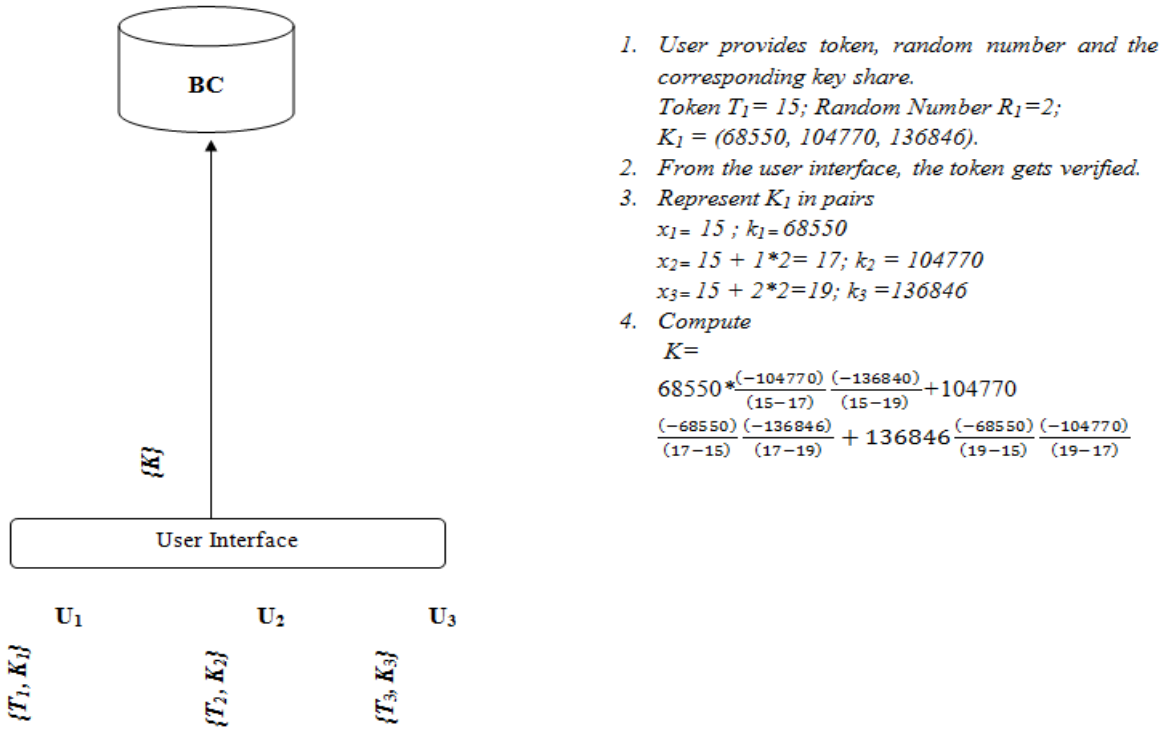

Figure 5: Decryption Phase

REFERENCES

[1] Amos Fiat; Moni Naor (1994). "Broadcast encryption". Proc. Advances in Cryptology – CRYPTO '93 (Extended abstract). Lecture Notes in Computer Science. 773: 480–491.

[2] Michael Luby; Jessica Staddon (1998). "Combinatorial Bounds for Broadcast Encryption". Proc. Advances in Cryptology – EUROCRYPTO '98. Lecture Notes in Computer Science. 1403: 512–526. doi:10.1007/BFb0054150.

[3] Noam Kogan; Yuval Shavitt; Avishai Wool (May 2003). A Practical Revocation Scheme for Broadcast Encryption Using Smart Cards. 24th IEEE Symposium on Security & Privacy (Extended abstract).

[4] G. H. Chiou and W. T. Chen, Secure Broadcasting using the Secure Lock, IEEE Trans. on Software Engineering, vol 15, 1989, pp. 929–934.

[5] C. Laih, J. Lee and L. Harn, A New Threshold Scheme and its Application is Designing the conference Key Distribution Cryptosystem, Information Processing Letters, vol 32, 1989, pp. 95–99.

[6] J.A. Garay, J. Staddon and A. Wool, Long-Lived Broadcast Encryption. Advances in Cryptology CRYPTO'2000, Lecture Notes in Computer Science, vol 1880, pp. 333-352, 2000

[7] Dalit Naor; Moni Naor; Jeff Lotspiech (2001). "Revocation and Tracing Schemes for Stateless Receivers". Proc. Advances in Cryptology – CRYPTO '01. Lecture Notes in Computer Science. 2139. pp. 41–62. doi:10.1007/3-540-44647-8_3. ISBN 3-540-42456-3.

[8] Halevy, Dani and Adi Shamir. "The LSD Broadcast Encryption Scheme."Advances in Cryptology (Crypto 2002). Lecture Notes in Computer Science 2442. Springer-Verlag.

[9] D.Naor., M. Naor, J. Lotspiech, Revocation and Tracing Schemes for Stateless Receivers. February, 2001.

[10] Scott C.-H. Huang; Ding-Zhu Du (March 2005). "New Constructions On Broadcast Encryption and Key Pre Distribution Schemes". Proc. IEEE Computer and Communications Societies – INFOCOM 2005. 1: 515–523. doi:10.1109/INFCOM.2005.1497919.

[11] Yevgeniy Dodi ,Nelly Fazio" Public Key Broadcast Encryption for Stateless Receivers "ACM Workshop on Digital Rights Management, 2002 - Springer.

[12] Norranut Saguansakdiyotin and Pipat Hiranvanichakorn" Broadcast Encryption Based on Braid Groups"

[13] IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012

[14] A. Muthulakshmi, R. Anitha "Identity-based broadcast encryption for multi-privileged groups using Chinese remainder theorem"Int. J. Information and Computer Security, Vol. 6, No. 3, 2014.

[15] N.-S. Jho, J. Y. Hwang, J. H. Cheon, M. Kim, D. H. Lee and E. S. Yoo, One-way chain Based Broadcast Encryption Scheme, In Advances in Cryptology-Eurocrypt 2005, Springer, LNCS vol. 3494, pp.559-574, 2005

[16] Xingwen Zhao, Fangguo Zhang and Haibo Tian, "Dynamic asymmetric group key agreement for ad hoc networks", Ad Hoc Networks, Vol.9, pp.928–939, 2011.

[17] A. Shamir, Identity-based Cryptosystems and Signature Schemes, Proceedings of CRYPTO '84, LNCS 196, pages 47-53, Springer-Verlag, 1984.

[18] Kaya K, selçuk A A (2008) A verifiable secret sharing scheme based on the Chinese reminder theorem . In: chowdhury D R., Rijimen V., Das A.(eds) Progress in cryptology-INDOCRYPT 2008. INDOCRYPT 2008. Lecture Notes in Computer science , Vol 5365. Springer, Berlin, Heidelberg.