IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331,
PP 38-42
www.iosrjournals.org

A Survey on Broadcast Encryption

Ginu Saju[1], Deepika M.P[2]
[1]*(PG Student ASIET, Kalady,India)*
[2]*(Associate Professor ASIET Kalady, 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, how a few different broadcast encryption schemes work, their merits and demerits.*

Keywords: *Broadcast encryption, Braid groups, Asymmetric group key agreement, Dynamic asymmetric group key agreement*

I. 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 shop networks, which each node in these networks has limitation in computing and storage resources.

In practice most BE 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).

II. Broadcast Encryption

A. Fiat and M. Naor [1] first proposed the concept of broadcast encryption in 1993.Broadcast encryption (BE) is a cryptographic method for a center to efficiently broadcast digital contents to a large set of users so that only non revoked users can decrypt the contents .In broadcast encryption the center 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 center 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 center broadcasts:

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

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 [5] proposed the notion of *long-lived broadcast encryption* schemes,

Whose purpose is to adapt to the presence of compromised keys and continue to broadcast securely to privileged sets of users. Our 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 predefined 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.

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 proposed a way to extend the lifetime of a broadcast encryption scheme. They describe a system in which keys for devices are stored on smartcards. When a pirate decoder has been found, the keys associated with its smartcard will be revoked. A user's keys can also be revoked if her subscription expires. When all the keys in an innocent device have been revoked, its smartcard will have to be replaced with a new set of keys. Keys also need to be replaced if the contract for a given device has expired. 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.

Halevy, Dani and Adi Shamir [7] proposed *The layered subset difference (LSD) scheme*, enables each user to store one kilobyte worth of keys on a smart card and the broadcast center 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 [8] 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 to compress 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.

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 [7].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. Later, Nam-Su Jho, Hwang [1] proposed *One way chain based broadcast encryption schemes*. 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 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 any time, which is not possible in tree based schemes.

Norranut, Pipat[9] 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 Aggregately 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. 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 scheme. 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

National Conference on "Emerging Research Trends in Electrical, Electronics & Instrumentation" 40 | Page

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.

Our scheme is made up of three algorithms; setup, encryption, and decryption. In the setup phase, when any user needs to 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[10] proposed *Identity based broadcast encryption for multi-privileged groups using CRT* .Most group oriented applications require strict access control mechanisms to prevent un authorized 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 [4] 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 (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).

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.

III. Conclusion

In this paper, we got into Broadcast encryption and a review on broadcast encryption. Basic notions of broadcast encryption were talked. Afterwards, some of proposed schemes in broadcast encryption were investigated.

References

[1] S.Berkovits, How to Broadcast a secret, Advances in Cryptology - Euro-crypt'91,*Lecture Notes in Computer Science 547, Springer, 1991, pp.536-541.*

[2] M.Naor, A. Fiat, Broadcast Encryption, Advances in Cryptology - Crypto 93',*Lecture Notes in Computer Science 773, Springer, 1994, pp. 480-491.*

[3] E.Gafni, J.Staddon and Y.L. Yin, Efficient methods for integrating traceability and broadcast encryption, Proc. Advances in Cryptology - Crypto *'99, LNCS 1666, Springer, 1999, 372-387.*

[4] Shamir, A., "How to Share a Secret", Communications of the *ACM, vol. 22, NO.11, November 1979, pp. 612613*.

[5] 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*

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

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

[8] Yevgeniy Dodi ,Nelly Fazio” Public Key Broadcast Encryption for Stateless Receivers “ACM Workshop on Digital Rights Management, 2002 - Springer

[9] Norranut Saguansakdiyotin and Pipat Hiranvanichakorn” Broadcast Encryption Based on Braid Groups” IJCSNS International Journal of Computer Science and Network Security*, VOL.12 No.2, February 2012*

[10] 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*