ABSTRACT

The rapid progress in the technologies underlying multicast networking has led to the development of many group oriented applications, such as pay–per-view, online teaching, teleconferencing and communal gaming. In these applications group members subscribe to different data streams and members have different access privileges. Security of group communications is achieved by encrypting the messages using a group key that allows the users of that group alone to decrypt a broadcast message. Group key has to be updated when there is a change with membership to preserve forward and backward secrecy. As the size of the group grows and/or the rate of membership change increases, the frequency of rekeying becomes the primary bottleneck. Also in group oriented applications, traditional multicast key management schemes are not sufficient to handle issues associated with multiple services.

In multi-privileged groups, multiple data streams are to be broadcast to the users based on their privileges. A broadcast encryption is a cryptographic primitive that enables encryption of broadcast contents such that only a set of targeted users, can decrypt the content. In Identity Based Encryption (IBE), users identifier information can be used as public key, which significantly reduces the need for certificates in Public Key Infrastructure (PKI), and it poses threat to user privacy. In applications like Military field, the list of receivers who receive a command should not be disclosed. Otherwise, when a single receiver is trapped, the identities of all the users are revealed. In broadcasting applications like pay-per-view channel, commercial websites the identity of the users should not be revealed, in order

to avoid targeted advertisement. Hence in addition to access control, the users identities also need to be confidential in some systems.

The objective of this thesis is twofold, key management and broadcast encryption in multi-privileged groups. One of the aims is to reduce the rekeying cost when multiple users join, leave or switch in multi-privileged groups. The next aim is to provide efficient broadcast encryption schemes with multiple data streams intended for different groups of users.

In existing batch rekeying, the key server waits until a rekeying interval T, and then it generates new keys, constructs the rekey message and multicasts or unicasts the same. When T is small, rekeying has to be done frequently whereas for a large T, the waiting time of users increases. This problem is addressed in **Chapter 2**, which gives a scheme for multiple user join/leave case in multi-privileged scenario with min(N, T) policy. The merging and rekeying operations are initiated following M/G/1 queueing model with min (N, T) policy. The key server waits for the arrival of at most N users or the elapse of T time whichever occurs first to start merging and rekeying in case of join/leave. A key graph representation for multi-privileged group is considered and the service groups are maintained as binary trees. Algorithms for multiple user join, leave and batch balancing have been discussed and an analysis is done for the rekeying costs.

In a binary key tree, the number of nodes of key encryption keys that are getting affected when a new user joins the key tree increases with the height of the key tree, which in turn increases the number of multi-cast messages to be sent to the existing users. Hence higher order trees and height balancing techniques are needed to maintain the key trees as balanced. Even with higher order trees like B-trees, the problem still pertains, since there is node splitting during user join. In a Non-Split Balancing Higher-Order

(NSBHO) tree, node splitting is avoided by the use of a special path and the tree grows upward without disturbing the existing users much, in case of new user join and thereby reduces the number of multicasts. **Chapter 3** proposes schemes using NSBHO tree for multiple users join, leave and batch balancing and analysis for rekeying costs in each case.

Chapter 4 presents an Identity Based Broadcast Encryption (IBBE) scheme preserving user identities based on Twin-Diffie Hellman problem and Homomorphic encryption. An IBBE scheme using homomorphic encryption to send multiple data streams to the selected set of users in multi-privileged groups is constructed. The scheme achieves forward secrecy and backward secrecy and resists collusion attack. But the size of the cipher text produced by this scheme is linear in the number of users and the issue with the size of the cipher text is rectified in the next chapter.

In **chapter 5**, a scalable identity based broadcast encryption scheme for multi-privileged groups is developed using Chinese Remainder Theorem and Bilinear Pairing. In the proposed scheme, a system of congruences is generated using keys obtained through bilinear pairing, the system is solved using Chinese Remainder Theorem and the solution is broadcast to the users. A valid user can obtain the session key from the solution and decrypt the message intended for him. The system preserves both forward and backward secrecy. The main advantage of the scheme is, it produces constant size cipher text for a service group.

The IBBE schemes in fourth and fifth chapters are proved to be IND-CCA secure for confidentiality and ANON-sID-CCA for anonymity under random oracle model. Performance comparisons of these schemes with some of the existing schemes reveal that the proposed schemes are highly

efficient. Of the two proposed IBBE schemes, the one in chapter five is efficient in terms of scalability and computations.

In some applications, it is desirable to encrypt the contents without exact knowledge of the set of intended receivers. Attribute based encryption offers this ability and enforces access policies defined on attributes, within the encryption process. In these schemes, the encryption keys and/or cipher texts are labeled with sets of descriptive attributes defined for the system users, and a particular user private key can decrypt only if the two match. **Chapter 6** presents an attribute based broadcast encryption scheme for multi-privileged groups, whose security depends on Decisional Diffie – Hellman problem and Decisional Bilinear Diffie – Hellman problem under random oracle model. This scheme achieves constant ciphertext size for each service group.

In this study, some issues related to key management and broadcast encryption in multi-privileged groups are analyzed and schemes are proposed to overcome those issues. A key management scheme is developed for multi-privileged groups to reduce, the waiting time of the users by using min(N,T) policy for batch rekeying. A key management scheme using Non-Split Balancing Higher Order (NSBHO) trees that reduces the number of multicasts during each rekeying is developed. Two Identity Based Broadcast Encryptions (IBBE) , the first using Twin-Bilinear pairing and homomorphic encryption and the second using Chinese Remainder Theorem (CRT) and bilinear pairing , both preserving identities of users have been proposed. An Attribute Based Broadcast Encryption (ABBE) scheme which follows ciphertext policy has been proposed. Over all, this study reduces rekeying costs in the key graph and provides some efficient broadcast encryption schemes for multiple data streams.