Enhanced Arbitrary Topology Generalization and Broadcast Encryption with W-RGK Scheme

R. Rasi Raj*
Department of CSE, Francis Xavier Engineering College, Vannarpettai, Tirunelveli-627003
***Corresponding author: E-Mail: rasirari@gmail.com**

ABSTRACT

The sender securely transmit messages to a strong altered set of users over an unpredictable channel is known as Broadcast encryption. The advanced encryption method demands a trusted party to distribute decrypted keys. A Group of Members are creates with the help of Group Key Agreement protocols which is used for the unknown accessing of decrypted text is avoid by generating the common encryption key through the open networks. And the Contributory Broadcast Encryption (Con BE) worked together with GKA and enable the sender to issue message to a appropriate member of the group although, it refuse to offer a fully trusted third-party to organize the system. Existing GKA protocols cannot control sender/member changes effectively. The method contains Master Secret Key which is controlled by Private Key Generator. The PKG improves the distributing the information of decryption keys to users and public broadcast encryption key. The proposed scheme is Enhanced Arbitrary Topology Generalization and Broadcast Encryption W-session Reliable Group Key management (W-RGK). The basic mechanisms of the proposed scheme can be described as a key update followed by a join and a leave operation with key recovery. The time between two consecutive member change operations as a session is termed. The group key is updated on a session change. Thus, the lifetime of a group key for a session is the same as the duration of the session. It face a mechanism to grant proper receivers to identify the current group key, even if they forget the key renew messages for long-term sessions.

KEY WORDS: Group Key Agreement, Contributory Broadcast Encryption, Broadcast Encryption, Private Key Generator, Master Secret Key, Reliable group key management, W-RGK.

1. INTRODUCTION

Network security is designed to preserve the applicability and integrity of our network data and it consists of the policies and habits maintain to avoid and monitor unauthorized access, alteration, misuse, or denial of services of a computer network and network usability resources. Network security consists of network administrator and which controls the authorized access of data. Also it covers various computer networks, both public and private, that uses in daily jobs, handle transactions and information exchange among businesses, government agencies and individuals. Broadcast encryption is mainly based on cryptography method and it forwarded the encoded information over a broadcasting channel. The method is very much important when secret sharing method through private keys. Broadcast encryption manages a large number of receivers at a time and but only the selected receivers can decoded the sender's message.

Broadcast encryption method broadcast same messages to all the users and these users in the group find out the messages during any other derived silliness or not anything at all group of users and key distribution center are the main parts of the broadcast encryption. W-RGK scheme is collusion resistance by defining an attacker who can fully control all the members outside the intended receivers but cannot extract useful information from the cipher text. The scheme involves a RGK.

Related Work: Abdalla (2010), introduced the GKE +P & GKE+S Protocol from modifies PDHKE and providers différent session Key. This technique is very much efficient and compare the performance of both Protocol by using Gap Diffie – Hellman (DH) assumption. Group Key Exchange +Protocol os not secured as compared to mBD+P.

Lewko (2010), introduced the flexible security under the Attribute Broadcast Encryption (ABE), d- Binary DH and also the Decisional Linear premise. Selectively protects in usual models under new non- interactive assumption. The advantage is capability of ABE scheme and disadvantage is that it decreases considerably with the use of large network formation. Liu (2010), discussed about the three different attack models provide. This technique is mainly helps to form large-scale tiny networks and monitors network traffic. It doesn't use in random graph processes.

Phan (2011), used a group of five protocols or algorithms DBE (set up, key gen, join, encap, decap). This scheme required the communication between all the group members and each time a new user wanted to join then it has to send request first. The main disadvantages of this technique are the interaction with all the users it delayed. And also can't handle sender change efficiently.

Jarecki (2011), developed the two round Group Key Agreement (GKA) protocol which secures under the decisional square DH assumption. The extended robust GKA and Diffie-Hellman helps to avoid the attack by the inside malware. It only works in the single hop or unidirectional links.

Michael Scott (2011), proposed Attribute based Broadcast Encryption and it use type1 &type2 elliptic curves. This technique is most efficient because it include many secured protocols.

Ruxandra and Olimid (2011), developed a technique which has a credible key generation center that includes a replay operation which avoids normal attacks in Group Key Transfer (GKT) protocols. And also various protocols provided to support this function. It can afford more security, Denial of Service (DOS) and secret sharing is impossible. There is no security proof for the secure GKT protocols.

Akhil Kaushik and Satvika (2013), uses an Extended Daffier – Hellman Algorithm (XDHA) and random number generation of the image. The main disadvantages of this technique are the use of discrete logarithm and man-in-middle attackers.

Jintai Ding, Xiaodong Lin (2014), proposed a Ring Lattice Based Key Exchange with Learning with Errors (RLWE) and Diffie – Hellman algorithms are used. It is robust, occurred small errors and don't support non – commutative rings.

Newlin (2014), proposed the Multi- Authority Attribute Based Encryption (MA- ABE) scheme and design an Attribute Based Key Generation Algorithm (AB-KGA) that helps to compare sizes. It develops efficient multi-authority attributes based encryption system. It is not efficient and non-existences of attribute revocation mechanism.

Boneh (2014), construct the ABE for arithmetic short keys and use point- to- point algorithm. Build FKHE from LWE. Multiple gates can handle at a time, more secure and efficient. A wireless system can't applicable in this technique because it is a circuitry system.

David Adrian (2015), using an Export Grade Diffie – Hellman Algorithm or SSH & IPSec. It attacks the TCS and uses VPN decryption method. The technique is understood by system builders and shared into groups also some few keys are exchanged. XDHA is more advantageous than EG- DH and less secure.

Qianhong Wu (2015), proposed the Contributory Broadcast Encryption (ConBE). The ConBE enable the sender to transmit a text or message to an appropriate participant of the group. ConBE method that contain a short cipher text proved to be completely collusion-resistant over the decision ŋ-Bilinear Diffie- Hellman Exponentiation (BDHE). This standard model also include aggregate Broadcast Encryption scheme.

Ankush and Avinash (2016), proposed the Contribute Broadcast Encryption (Con BE). This encryption method uses elliptic curve cryptography that increases the efficiency. This includes three main disadvantages. They are, it have small key sizes and difficult to justify and single hop is used.

Rasi Raj and Joy (2016), discussed the Identity-Based Broadcast Encryption (IBE) scheme with various topology generalization that provides more secure encryption and decryption of the messages. IBE is totally secured as a result of each receiver has its own unique ID. The Private Key Generator (PKG) is acting as a base node, the keys are exchanged, this encrypted key is used for data transmission and extended Proxy Re-encryption method includes to providing for collusion resistant mainly proxy re-encryption is used for Expanded Filtering of Encoded Spam and secures the file systems are modelled one by one. The encryption and decryption depend on the private parameters, Master Secret Key (MSK) and identities that are generated by the PKG.

2. MODELLING TOPOLOGY GENERALIZATION AND BROADCAST ENCRYPTION (TG-BE)

The proposed method can be described as a key refreshing followed by a join and a leave operation with key recovery. The basic operations of the scheme are explained as a key update followed by a join and a leave from the group with key recovery. The time between two consecutive member change operations as a session is termed. The group key is updated on a session change. Thus, the lifetime of a group key for a session is the same as the duration of the session. The basic mechanisms of the proposed scheme can be described as a key update followed by a join and a leave operation with key recovery. The RGK is the major building block in broadcasting and there are any other protocols to alternate its properties. Arbitrary topology generalization provides multi-hop or bidirectional link connection. It is collusion- resistant and avoids the neighboring communication problems. The method involves a Private Key Generator (PKG) with RGK. The PKG provides private keys for users' and identities by using a Master Secret Key (MSK). PKG also provides the distribute information of decryption keys to users and public broadcast encryption key. Suppose that the system users are $U = \{U_1, U_2, \ldots, U_n\}$ where $n > 1$ and $n \in 1$. Each user U_i has a corresponding identity ID_i. This scheme consists of a group of algorithms such as Parameter Generation, Extract, Setup, Encrypt, Proxy re-encryption and Decrypt described as follows:

Parameter Generate (λ', n'): This input the secured parameter λ' and n' the whole number of the users and outputs a MSK and a group of system parameter Φ. The MSK is saved secret by PKG.

Extract (MSK, ID_i): This algorithm is run by using the help of PKG. That input the MSK and a user U_i's identity ID_i, and outputs the user U_i's private key s_i.

Setup (MSK, Φ, U): This algorithm provides the PKG, that takes as input the MSK, the system parameters Φ and $U = \{U_1, U_2, \ldots, U_n\}$, and outputs the decryption key dk_i for each user $U_i \in U$ $(1 \leq i \leq n)$.

Encrypt (Φ, R, PK, M): This algorithm uses a sender who knows the public encryption key. It takes as input the system parameters Φ, a group of receivers R {1, …, n}, the public encryption key PK and the any message Mn to be encrypted, and get a Cipher Text C'. Then the sender broadcasts (c, R) to the system users.

Proxy Re-encryption (Pe, pk, sk): The proxy re-encryption captures B's protection, also when the Proxy (with the knowledge of all re-encryption keys). A group of assigned users (with the knowledge of their own secret keys) plot

against B and provided that B never delegated decryption rights to any adverted user. pk and sk are Private Key and secret key.

Decrypt (Φ, R, U_j, dk_j, s_j, c): This input system consists of parameters Φ, the Private Key s_j, the receiver set R, a receiver U_j ($j \in R$), U_j's decryption key dk_j and the cipher text c. It then outputs the original plain message M.

Formation of network: The nodes are deployed in the Network Animator and the area is1500 x 1500. The parameters such as transmission range, frequency, antenna type, routing protocol and security schemes. The source and destination nodes are declared. Here we calculated the source to destination route.

W session Reliable Group Key Management (W-RGK) Protocol: Let U = {u1,…., un} is the universe of the users, and i ∈ N be an index to represent a session. The GM is in charge of a key server in the proposed protocol, thus we will use them interchangeably henceforth. Let skit be the set of secret keys of user ut ∈ U at session i, and GKi be the group key at session i. During the initial setup (session 0), every user ut ∈ G0 receives sk0 t and GK0 from GM in a secure and reliable manner. This can be achieved during in the initial registration or installation of the device for the multicast service by manual means. When a member joins or leaves the group at session i, the session changes from i to i + 1 and secret/group keys are updated and delivered to the valid group members using the key update protocol for backward or forward secrecy.

Key exchange: Key exchange module allowed any two parties that doesn't have any prior knowledge of another one to jointly provide a shared secret key over an uncertainty channel**.** This key is also used to encode subsequent exchange of information using a symmetric key cipher. This key will be distributed to users by the Private Key Generator.

Broadcast encryption with W-RGK scheme: A W-RGK is mainly used when the key updated with each session and session change when one party complete the transmission process. The key also get updated when the contents of messages transferred to the second party and encrypted by using its public key to a third party, without revealing his private key of the first party. Two functions are Delegation that allows any message content (key holder) to produce the re-encryption key relied on the Secret Key and key of authorized user. This re-encryption key with W-RGK is uses above the proxy as input to re-encryption operation and that is accomplished by the proxy to decode the cipher text to an authorized user's key. And the second function is Transitive W-RGK is helped refresh the key updating with session change, also control group leaving and joining process and PRE method that allows the cipher text to be re-encrypted in an unlimited number of times.

Data transmission: The sender will transmit the data packets to receiver's side using encryption process. Encryption is the method of encrypting information or messages and this method is used for reading the content only by the authorized parties. In the encryption method, the appropriate exchange of information or messages that are offered to as plaintext and it is encrypted using an arbitrary topology generalization and broadcast encryption with W-RGK scheme. Then generating cipher texts that can one self to be read when it is decrypted. The receiver will decode the message or data using that secret key.

Proposed Broadcast Encryption with W-RGK: W-session Reliable Group Key (W-RGK) distribution method is used with various topology generalization and Broadcast Encryption. It controls access to the streaming multimedia broadcasts, when the above mentioned constraints exist. The proposed scheme features small key refresh the messages and w-session reliability. The proposed scheme describes an operation that allows appropriate receivers that to figure out the ongoing group key using short hint messages and member computation, while they lost key refreshing messages for long-term sessions. It is Collusion-resistance which is defining the attackers that can totally control every group members outside the pre-determined receivers but also it cannot extract the important information from the cipher text. This scheme involves PKG and it contains MSK which provides the private keys from user's identities. The public BE key and distributes information of decryption keys to users are controlled by PKG. Suppose that the system users are U = {U_1, U_2, …., U_n} where n > 1 and n ∉ 1. Each user U_i has a corresponding identity ID_i. In fig.1, describes that the session changes detaily.

Parameter genereate (λ, n): Assumes that total numbers of group members are n and λ is the security parameter. The ATIBE parameters are; π = (λ, n, MSK, {U_1, U_2, …., U_n} , ϕ)

Extract (MSK,IDi): Combine the MSK and IDs of each user. The algorithm is run by PKG when the user requests their private key. It take input π, MSK and ID ε {0,1}*and returns the private key d for user ID. Setup (MSK, ϕ, U): MSK: the MSK is generated by PKG, irregularly choose key value 1,..., n and give individual IDs to each user. PK= msk + ID + sender Hello.random + recipient Hello.random

Private Key, sk= IBE (secret, ui−1)

Consider j=1,.., n and decode key the user j.

dk_j =($\sigma_1 j$, … … . , σ_nj)

$\sigma_i j$=XiUj, X ε G

Output=u1, u2, ⋯

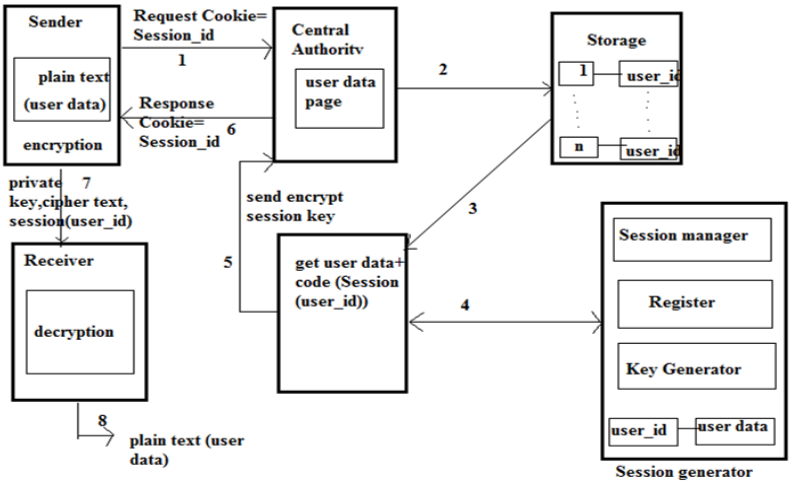

Figure.1. Broadcast Encryption and W-RGK Scheme

Encrypt (Φ, R, PK, M): Takeπ. The inputs are system parameterϕ, n number of receivers R=1,...n, public key PK and plain message M. $C_M$is cipher text or output of the encryption;

C_M=,π, encrypt (π,M,ID)

Decrypt (Φ, R, U_j, dk_j, s_j,C_M): Accept d, π,$C_M$and return M.

M, ID ε {0,1}* :

dk_j =decrypt (extract (π,MSK,ID) ,π, encrypt (π,M,ID)) = M

Proxy Re-encryption (Pe (PK, sk): C_M=enc (PK, M) into a new ciphertext C_M' which is decrypted into decryption (sk', C_M'). Do the above process without direct decryption, actually virtually decrypt C_M in the draft chamber guarded by PK'. The processes are following:

- Generate $\bar{sk}_i$ = enc (PK', sk_i) Where sk_i denotes the i-th bit sk.
- Compute $\bar{C}_{Mi}$= enc (PK', $\bar{C}_{Mi}$) Where C_{Mi} denotes i-th bit.
- Evaluate the decryption circuit is C_M'= eval (PK', sk_1',...,sk_n', $\bar{C}_{M1}$,…, $\bar{C}_{Mn}$)

Then the decryption become, Dec(sk',C_M')=dec(dec($\bar{sk}_i$),..,dec($\bar{sk}_n$),dec(sk),...,dec(sk')

= dec(sk_1,..., C_{M1},....., C_{Mn})=dec(sk, C_M) = M

3. SIMULATION RESULT

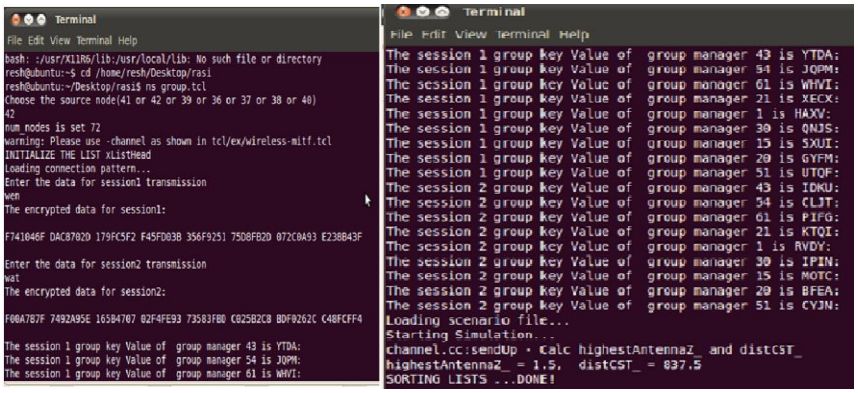

Figure.2. Data encryption for session 1 and session 2 &their group key values

Fig.2, shows the data encryption for session 1 and session 2 and their group key values. Number node used is 72 and enter the data for both session 1 and session 2 transmission. After entering the data each data encrypted. Both sessions have different group key values. The session 1 and session 2 group key values for appropriate Group Manager (GM). The group key values changes for each session change. The encryption of the data depends on these group key values.

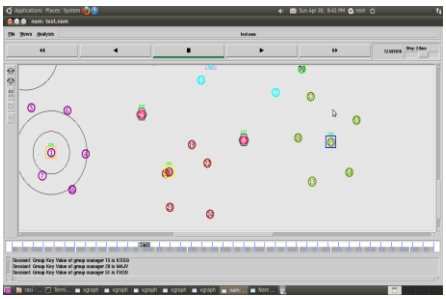

Figure.3. Group formation

Fig.3, shows the group formation. Nine groups are formed, each group has one Group Manager (GM) and data transmit one group to another group via Gateway (GW). The group managers change its session key values after every execution.

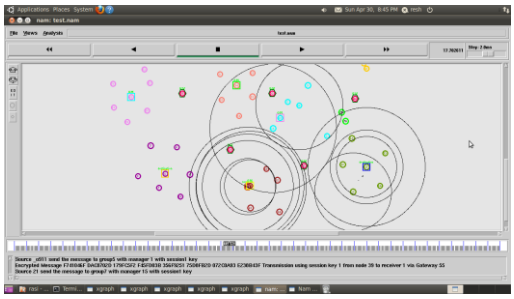

Figure.4. Encryption process

Fig.4, represents the text message sent from source node to destination node via the respected group of nodes. Destination node decrypts and reads the message. Arbitrary Topology Generalization and Broadcast Encryption with W-RGK Scheme is used, for group key agreement protocols run purely on an open radio medium, if all members are within easy radio range, then members' relative spatial arrangement and positions on a given topology are somewhat unimportant.

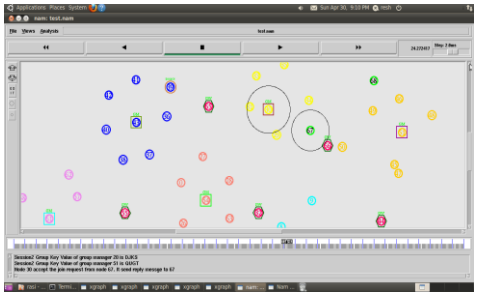

Figure.5. Node joining process

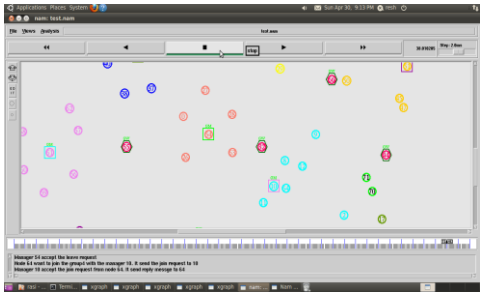

Figure.6. Node leaving process

Fig.5 and fig.6, shows node leaving and joining process. Efficient rekeying and lost key recovery is used. High level of reliability and security, while guaranteeing lower communication overhead compared to previous reliable group key distribution schemes recovery for stateless receivers. Let U = {u1,…., un} be the universe of users, and i ∈ N be an index to represent a session. Let GM be the group manager, and Gi ⊂ U be the communication group that consists of legitimate group members in session i. The group manager is in charge of a key server in the proposed protocol, thus we will use them interchangeably henceforth.

Figure.7. The execution time of BEncrypt and BDecrypt

Fig.7, represents the execution time of broadcast encryption and decryption. The number of nodes and execution time plotted along the x-axis and the y-axis.

4. CONCLUSION

The Arbitrary Topology Generalization and Broadcast Encryption with W-RGK scheme can handle sender/member changes efficiently, and provides a completely credible third party to establish the system or network. The MSK is used in the PKG for identifying the user's private key. This avoids the neighbors' communication problem, efficient encryption/decryption and only one round is needed to establish the public group. The operations propagate over the network along the spanning tree. AT-GIBE is used in any connected network topology with bidirectional links because a spanning tree can always be manufactured in any network. W-RGK scheme is used. The basic mechanisms of the proposed scheme can be described as a key update followed by a join and a leave operation with key recovery. The time between two consecutive member change operations as a session is termed. The group key is updated on a session change. Thus, the lifetime of a group key for a session is the same as the duration of the session. The basic mechanisms of the proposed scheme can be described as a key update followed by a join and a leave operation with key recovery. The time between two consecutive member change operations as a session is

termed. The group key is updated on a session change. Thus, the lifetime of a group key for a session is the same as the duration of the session.

In future different channel properties and different topologies need to be investigated to discover further useful interactions. As multiple channels may increase overheads, studies could be done to consider best topology combinations to achieve high security at the least expense. Instead of RGK protocol can be also formalize new protocols.

REFERENCES

Abdalla M, Chevalier C, Manulis M and Pointcheval D, Flexible Group Key Exchange with On- demand Computation of Subgroup Keys, in Proc. Africa crypt 2010, vol. LNCS 6055, Lecture Notes in Computer Science, 2010, 351-368.

Akhil Kaushik and Satvika, Extended Diffie - Hellman Algorithm for Key Exchange and Management, ICETEM, 2013.

Ankush Ajmire V, Avinash Wadhe P, Anonymous Key Generation Technique with Contributory Broadcast Encryption, International Journal on Recent and Innovation Trends in Computing and Communication, 4 (5), 2016, 277 – 281.

Boneh D, Gentry C, Gorbunov S, Halevi V, Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits, in Proc. Eurocrypt 2014, LNCS Lecture Notes in Computer Science, 8441, 2014, 533-556.

C´ecile Delerabl´ee, Identity-Based Broadcast Encryption with Constant Size Cipher texts and Private Keys, Kurosawa K, (Ed.): ASIACRYPT 2007, LNCS 4833, c International Association for Cryptology Research, 2007, 200–215,

David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Imperfect Forward Secrecy, How Diffie-Hellman Fails in Practice, CCS'15, October Denver, Colorado, USA, 2015, 12–16.

Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger, Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage, 12th Annual Network and Distributed System Security Symposium (NDSS), 2005.

Ruxandra F, Olimid, On The (In) Security of Group Key Transfer Protocols Based on Secret Sharing, Proceedings Of The Romanian Academy, 14, 2013, 378–387.

Jarecki S, Kim J and Tsudik G, Flexible Robust Group Key Agreement, IEEE Transactions on Parallel Distributed Systems, 22, 2011, 879-886.

Jintai Ding, Xiaodong Lin A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem, citeserx, 4, 2014.

Lewko A.B, Sahai A, Waters B, Revocation Systems with Very Small Private Keys, in Proc. IEEE S & P 2010, 2010, 273-285.

Liu Z, Ma J, Pei Q, Pang L and Park Y, Key Infection, Secrecy Transfer and Key Evolution for Sensor Networks, IEEE Transactions on Wireless Communications, 9 (8), 2010, 2643-2653.

Newlin Rajkumar M, Ancy George, Brighty Batley C, An Overview of Multi-Authority Attribute Based Encryption Techniques, International Journal of Advanced Research in Computer and Communication Engineering, 3 (9), 2014.

Duong Hieu Phan, David Pointcheval and Mario Strefler, Security Notions for Broadcast Encryption, LNCS 6715, 2011, 377–394.

Phan D.H, Pointcheval D and Strefler M, Decentralized Dynamic Broadcast Encryption, in Proc. SCN, LNCS 7485, Lecture Notes in Computer Science, 2011, 166-183.

Qianhong Wu, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Oriol Farras, and Jesus A. Manjon, Contributory Broadcast Encryption with Efficient Encryption and Short Cipher texts, IEEE Transactions On Computers, 2015.

Rasi Raj R, Joy Winnie Wise D.C, Enhanced Arbitrary Topology Generalization and Identity-Based Broadcast Encryption, International journal for Research in Science and Engineering Technology, 3 (11), 2016.

Michael Scott, On the Efficient Implementation of Pairing-Based Protocols, In Chen L.(eds) Cryptography and Coding, IMACC, 2011, 296-308.