Turkish Journal of Computer and Mathematics Education Vol.12 No. 5 (2021), 984-988

Research Article

Hybrid Broadcast Encryption and Group Key Agreement Protocol with Precise Cipher Texts

Chinnala Balakrishna[a], Dr. Tryambak Hirwarkar[b]

[a]Research Scholar, Department of Computer Science and Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal-Indore Road, Madhya Pradesh, India.
[b]Professor, Research Guide, Department of Computer Science and Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal-Indore Road, Madhya Pradesh, India.

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: In cryptographic system so as to manage the group of members, the group key management protocol is used and it also should provide the security to the group of members which means the communication among the members will be done in secure manner. Broadcast Encryption (BCE) provides a key it arise common for all the members in the group during the encryption and all the associated members can decipher the message with the same mutual key but cannot stop decrypt the message by individuals. Broadcast encipher algorithm sends a secure transmit note to the entire members with the distributed key to decrypt the message with trusted third party. The conventional BE scheme fully relies on third party reliable key generator server machine, the responsibility of the third party server is to generating the undisclosed deciphering keys for the entire collection members and the group members are responsible for decrypt the messages which are encrypted under a common encrypted key. The purpose of Group Key Accord (GKAP) protocol is for negotiate all the assembly members and designing a familiar encryption key through the network. With the GKAP the group members are responsible for generating universal encipher key and it permits simply the group people to decrypt the cipher text which is encrypted by group members by using the shared encryption key but this GKA protocol it is not possible to exclude any members from the group to decrypt the cipher text shared under the common encryption key. In this paper we will combine these two techniques to produce a novel approach called as the Hybrid Broadcast Encryption (HBCE). In this innovative primeval all the cluster of participants agree and produces a widespread encipher key but though each individual having their own decipher key, So that the sender by looking the encryption key he will bound the deciphering to limited members for his abundance.

Keywords: Group Key Agreement Protocol (GKAP), Broadcast Encryption (BCE), Hybrid Broadcast Encryption (HBCE), Broadcast Aggregatable Encryption (BCAE).

1. Introduction

In the recent days there is a vast demand for group-oriented communications. In order to protect the group communications, the multipurpose cryptographic primitives will be used, there is also raising importance for multipurpose cryptographic techniques for computational platforms. The new computational tools are like instant messaging, group-oriented communications, social media and mobile ad hoc networks. These novel schemes are said to be cryptographic techniques. These cryptographic techniques are used by the sender to securely encrypt the information without fully depend on the trusted third-party technologies. Broadcast Encryption (BCE) [1] scheme is a well-known technique for the group-oriented communications. The working of Broadcast Encryption techniques is that the sender is broad cast the information to any subset of members with securely. However, this BCE System deeply depends on fully trusted third party technologies, these third-party technologies are responsible for generating the decryption keys for the entire cluster members.

The Group Key Accord Protocol (GKAP) is another type of encipher mechanism for communicating the group members in secure manner but we must ensure identity authentication, privacy, protection, and access control of information shared among the group members. The traditional GKAP [2] scheme is to enable the group of members for preparing the common secret key over the open networks but whenever a member of the group i.e sender willing to send the information to the group of members, first the sender mandatory to join into the group and apply the Group Key Accord Protocol for exchanging the undisclosed key among the intended members in the group. In order to defeat this pitfalls Wu et al. Invented an Asymmetric Group Key Accord Protocol [3], according to this technique the common group public key is prepared and all the remaining members holds different decryption keys. Both Conventional Symmetric Group Key and Asymmetric Group Key not having the capability to restrict any group member to read the basic text. Finally, this is vital to invent the further stretchy and efficient technique that should not fully depend on the trusted third-party key generation servers.

A. Contribution from Our Side

Here we proposed a innovative technology referred as Hybrid Broadcast Encryption, it is the hybrid technology of combination of BCE and GKAP. This primitive is a fully advanced, proven security mechanism with necessary illustrated experiments.

First we design a HBE scheme and formalize its definitions. HBE implements the features of both technologies like BCE and GKAP. All the group members are communicated over the network, they agree on a particular protocol for generating the common public key. However in this technique each member in the group including the sender having their own decryption keys for decrypting the message which is encipher by the sender after agree on every single one the cluster members in the cluster. Based on the public encryption key any member in the group has a right to encrypt the message of any subset in the group but only the members that are selected by the sender has the capability to decrypt the information. In the GKAP it is not possible to eliminate any from the group but in HBE it is possible to omit any member or subset of members from the group. Match up to Conventional Broadcast Encryption technique the Hybrid Broadcast Encryption technique not totally depends on the trusted third party servers.

The second one is to implement the concept of Broadcast Aggregatable Encryption (BCAE). The Broadcast Encryption is BCAE if it meets all the security measures of BCE primitive. Hence it is proven that the BCAE is a fully collusion free secure encryption system by implementing the concept of Diffie Hellman Key Exchange. Single round operation is enough for generate the unrestricted cluster encipher key and to place the HBCE scheme. Once the classification is established then it takes the storage cost O (m) this includes together the sender furthermore the remaining assemblage members in the group, here the m indicates all the group members.

B. Applications of HBCE

The HBCE is used to exchange the data among the social networks. According to the Prism scandal [4] all the members more likely to think about the security provided to their personal information shared to the other members through the social networks. The HBCE system can solve this problem. If any user want to exchange the information in the group without depending on the social network system, our scheme will give the solution to this problem.

For this system there is only one round required for any group member in order to send the information to the other persons, each associate sends the information to former associates in the cluster without waiting for the acknowledgements. After each and every member have received the other members information then they started sharing their encryption keys to one and all in the group. Because of exchanging the encryption keys this permits whichever sender to limited to share the information to any subset of members in the group.

C. Related Work

Several works have been done with respect to the BCE and GKAP. According to et al.[2][5] if this scheme is designed for m members then it is required O(m) rounds. Multiple round GKAP protocol expects synchronization in order to design the protocol. Several solutions have been addressed with respect to Time and Space complexity of a round, it will be studied in [6], [7], [8]. According to TZeng Constant GKAP protocol[9] it can easily identify the cheaters over the network. In order to deal the member change in the group Dynamic Group Key Accord protocols provides the scheme for this type of situations [10], [11] and [12].Wu et al invented a special protocol called Group Key Management protocol [13], it is clearly observed that changing of sender and if any person wants to quit in the group does not require any additional steps. Broadcast Encryption System will be dived into two categories depending on what type key is going to be used in the group. The first one is Single key or Symmetric key broadcast encryption [1] and the second on is Asymmetric or Public key broadcast encryption [14].If our system uses the Single key encipher scheme the trusted third party is accountable for producing and sharing the secret keys to all the other members in the group over the network.

2. Hybrid Broadcast Encryption and Group Key Agreement Protocol

We start by formalizing the HBE thought spanning the GKAP and the BCE natives. In HBCE scheme all the group members first mutually establishes a system and design a open encryption key, at this point the member who is responsible for sending the information can unreservedly choose the sub group, a sub group may be composed of gathering individuals, the members in the sub group are responsible for decode the cipher text.

Algorithm

This algorithm is composed of a Broadcast Encryption and Group Key Agreement Protocol defined as HBE scheme.
Step 1: Assign security parameter $\alpha \in N$
Step 2: define group members {A1, A2....., An}, here n is the positive integer
For entire members Ai, $1 \leq i \leq n$
Step3: Call HBE(ParamenterGenerator, HBEstablishment, HBEncryption, HB Decryption)
Step 4: ParameterGenerator(1α)
HBEstablishment(A1(t1),....,An(tn)), It is jointly run by the members A1,....,An, All the member of Ai receives the private input ti.
If (true)
Then Each Member A1 generates dki, where dki is the decryption key.
Else
Generates NULL
HBEncryption(R,PUgek): It is group encryption algorithm and it will be operated by the sender who is familiar with the PUgek(Public Group encipher key).It takes as input a receivers set $R \subseteq \{1,2,3,.....,n\}$ and PUgek and it generates output as pair of keys(c,¥),here c is the cipher text and ¥ is secrect session key,then after (c,R) is sent to the recipients.
HBDecryption(R,m,dkm,c): Deciphering algorithm is operated by each and every proposed receiver $m \in R$. This technique accepts put in as the receiver set R, index m, receivers decryption key dkm and the cipher text c, and one secret session key £ will be generated as a output.

3. An Aggregatable Broadcast Encrytption System (Aggbe)

The AggBE scheme is used to construct and implement the HBE schemes
A BE system includes the below algorithms.
BSetup(1α): This technique take a key in parameter α and it produces the output as group of broadcast receivers as say p, and a Broadcast encryption public/secret key pair(PUK,SEK).
BKeyGen(a,SEK): This algorithm takes the input as index i.e. $a \in \{1,2,3,.....,x\}$ and the secret key SEK and it produces private key (da) for user a as the output.
BEncryption(R,PUK). It takes the first parameter R, where R is the receiver set, $R \subseteq \{1, 2, 3, 4\cdots, x\}$ and the PUK, where PUK is called the Public key.
Step 1. If (R) > x, it will destroy the protocol.
Step 2.Else Check If $(R) \leq x$, it produces the result it is combination of (ct, μ) here the ct is referred as scrambled text and $\mu \in$ Key is the key for encrypting the information.
BCDecryption(R,a,da,PUK): In this Decryption step the algorithm permits all the receivers in the group to take the message encipher key μ through the cipher text. It takes input as a receive set S, the index a ε {1,2,3,.....,x}, the receiver's secret key da, the cipher text c and the public key PUK.
If (R) $\leq$ x and $a \in R$, then it produces the message encryption key as μ.

4. Performance Analysis and Results

For performance analysis we used the frequently adopted metrics for the conventional Broad cast Encryption scheme. The cost of the operations such as reading the receiver's identity and for simple quantification of group members will be taken into consideration.

After the Hybrid Broadcast set up procedure has done the sender should receive Public key and place it into the group GR. The group contains m members.

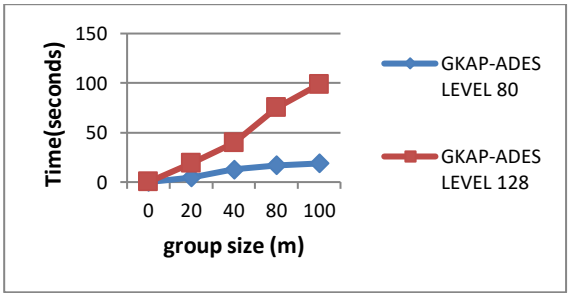

Figure 1. Execution Time for GKAP Using AES-80 and AES-128 Levels.

The above figure illustrates the execution time with respect to the group size by using AES-80 Level and AES-128 Level protocol. It is very clear that when the cluster volume is increasing the carrying out time and the security level also increased gradually.

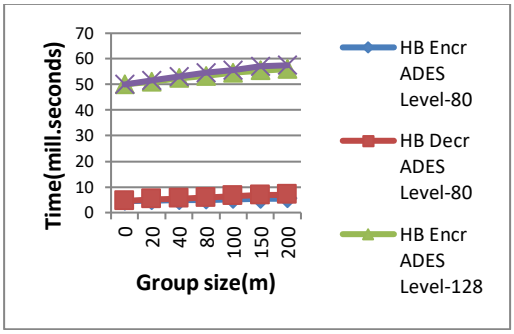

Figure 2. Execution Time for Encryption and Decryption Using AES-80 and 128 Levels

The above figure describes the session key. Here two operations are performed one is encryption and other is decryption for the session key. The execution time remains consistent while performing encryption and decryption to the session key over the network even for the different group sizes. It means if the group size is increased there is no change in the execution time. Here we applied Advanced Encryption Standard Level-80 and Level-128 also.

5. Conclusion

In this HBCE a member belongs to a group can send the information to all the members in a group or if it requires it possible to send to the subset of group. In this technique hence it is proved that it is completely avoids the trusted third-party key generation servers for generating the keys. So, we cannot completely depend on the third party servers. We can change the sender dynamically and also it is possible to add or delete the group members dynamically but it does not need extra rounds to generate the common keys in the group. The HBCE technique is a fully efficient and also it provides the security to the members in the group.

References

1. Park, J.H., Kim, H.J., Sung, M.H., & Lee, D.H. (2008). Public key broadcast encryption schemes with shorter transmissions. *IEEE Transactions on Broadcasting*, *54*(3), 401-411.
2. Wang, L., Guo, Y., Sun, Y., Zhao, Q., Lan, D., Wang, Y., & Wang, A. (2015). Synchronization-based key distribution utilizing information reconciliation. *IEEE Journal of Quantum Electronics*, *51*(12), 1-8.
3. Wu, Q., Mu, Y., Susilo, W., Qin, B., & Domingo-Ferrer, J. (2009). Asymmetric group key agreement. *In Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 53-170.
4. http://en.wikipedia.org/wiki/PRISM %28surveillance program%29, 2014.
5. Steiner, M., Tsudik, G., & Waidner, M. (2000). Key agreement in dynamic peer groups. *IEEE Transactions on Parallel and Distributed Systems*, *11*(8), 769-780.
6. Boyd, C., & Nieto, J.M.G. (2003). Round-optimal contributory conference key agreement. *In International Workshop on Public Key Cryptography*, 161-174.
7. Tzeng, W.G., & Tzeng, Z.J. (2000). Round-efficient conference key agreement protocols with provable security. *In International Conference on the Theory and Application of Cryptology and Information Security*, 614-627.
8. Zhang, L., Wu, Q., Domingo-Ferrer, J., Qin, B., & Dong, Z. (2015). Round-efficient and sender-unrestricted dynamic group key agreement protocol for secure group communications. *IEEE Transactions on Information Forensics and Security*, *10*(11), 2352-2364.
9. Li, J., Wen, M., & Zhang, T. (2015). Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks. *IEEE Internet of Things Journal*, *3*(3), 408-417.
10. Bresson, E., Chevassut, O., & Pointcheval, D. (2001). Provably authenticated group Diffie-Hellman key exchange—the dynamic case. *In International Conference on the Theory and Application of Cryptology and Information Security*, 290-309
11. Bresson, E., Chevassut, O., & Pointcheval, D. (2002). Dynamic group Diffie-Hellman key exchange under standard assumptions. *In International conference on the theory and applications of cryptographic techniques*, vol. LNCS 2332, Lecture Notes in Computer Science, 321-336.

12. Bresson, E., Chevassut, O., Pointcheval, & Quisquater, J.J. (2001). *Provably Authenticated Group Diffie-Hellman Key Exchange, In Proceedings on ACM CCS*, 255-264.
13. Wu, Q., Qin, B., Zhang, L., Domingo-Ferrer, J., & Manjón, J.A. (2012). Fast transmission to remote cooperative groups: a new key management paradigm. *IEEE/ACM Transactions on networking*, *21*(2), 621-633.
14. Naor, M., & Pinkas, B. (2000). Efficient Trace and Revoke Schemes. *In Proceedings on FC 2000, LNCS 1962, Lecture Notes in Computer Science*, 1-20.
15. Canetti, R., Halevi, S., & Katz, J. (2004). Chosen-Ciphertext Security from Identity-based Encryption. *In* Proceedings on EUROCRYPT 2004, LNCS *3027*, 207-222.
16. Matsuda, T., & Hanaoka, G. (2014). Chosen Ciphertext Security via UCE. *In Proceedings on PKC 2014, LNCS 8383, Lecture Notes in Computer Science*, 56-76.
17. Qikun, Z., Yongjiao, L., Yong, G., Chuanyang, Z., Xiangyang, L., & Jun, Z. (2019). Group key agreement protocol based on privacy protection and attribute authentication. *IEEE Access*, *7*, 87085-87096.