International Journal of Science Engineering and Advance Technology

Enhanced Arbitrary Topology for Efficient Encryption Using Short Cipher texts

Narsunaidu Bora[1], Dr. Rajendra Kumar Ganiya[2]
[1]M.Tech Scholar, Department of Computer Science & Engineering,
[2]Professor, Department of CSE, Sri Sivani College of engineering, chilakapalem, Srikakulam, AP, India.

Abstract:

The sender safely transmit messages to a dense changed concern of clients over an erratic channel is known as Broadcast encryption. The propelled encryption technique requests a trusted gathering to convey unscrambled keys. A Group of Members are makes with the assistance of Group Key Agreement conventions which is utilized for the obscure getting to of decoded is maintain a strategic distance from by creating the basic encryption key through the open systems. Furthermore, the Contributory Broadcast Encryption (Con BE) cooperated with GKA and empower the sender to issue message to a proper individual from the group in spite of the fact that, it decline to offer a completely put stock in outsider to compose the framework. The strategy contains Master Secret Key which is controlled by Private Key Generator. The PKG enhances the circulating the data of decoding keys to clients and open broadcast encryption key. The fundamental mechanisms of the proposed plan can be depicted as a key refresh took after by a join and a leave activity with key recuperation. The time between two back to back part change tasks as a session is named. The group key is refreshed on a session change. In this way, the lifetime of a group key for a session is the same as the term of the session. It confront a system to concede legitimate collectors to distinguish the present group key, regardless of whether they overlook the key reestablish messages for long haul sessions.

Keywords: Cryptography, Key Management, Group Key Agreement, Broadcast Encryption.

I. Introduction

With the expansion in innovation headway in correspondence advancements, there is an expanding interest of flexible cryptographic natives to secure group interchanges and calculation stages. These new stages incorporate texting instruments, community oriented registering, portable specially appointed systems and informal organizations. These new applications call for cryptographic natives enabling in two to safely encoding to any subset of the clients of the administrations without depending on a completely put stock in merchant. Broadcast encryption (BE) is an all-around examined crude planned for secure group-situated correspondences. It enables a sender to safely broadcast to any subset of the group individuals. All things considered, a BE framework vigorously depends on a completely trusted key server who creates mystery unscrambling keys for the individuals and can read every one of the correspondences to any individuals. Group key understanding (GKA) is another surely knew cryptographic crude to secure group-arranged interchanges. A traditional GKA enables a group of individuals to build up a typical mystery key through open systems. In any case, at whatever point a sender needs to make an impression on a group, he should first join the group and run a GKA convention to impart a mystery key to the planned individuals all the more as of late, and to defeat this confinement, with the presentation of hilter kilter GKA, in which just a typical group open key is arranged and each group part holds an alternate decoding key. In any case, neither regular symmetric GKA nor the recently presented topsy-turvy GKA enable the sender to singularly prohibit a specific part from perusing the plaintext. Subsequently, it is fundamental to discover more adaptable cryptographic natives permitting dynamic broadcasts without a completely put stock in merchant. This paper examines a nearby variety of the previously mentioned issue of one-round group key assention conventions and spotlights "on the best way to build up a secret channel sans preparation for different gatherings in one round". We give a short diagram of some new plans to comprehend this variety. Hilter kilter GKA Observe that a noteworthy objective of GKAs for most applications is to set up a

private broadcast channel among the group. We explore the probability to set up this divert in an awry way as in the group individuals only arrange a typical encryption key (open to assailants) yet hold particular mystery unscrambling keys. We present another class of GKA conventions which we name topsy-turvy group key assentions (ASGKAs),

II. Related Work

I. Ingemarsson, D.T. Tang and C.K. Wong, "A Conference Key Distribution System," IEEE Transactions on Information Theory, vol. 28, no. 5, pp. 714-720, 1982. Clarified that encryption is utilized as a part of a correspondence framework to shield data in the transmitted messages from anybody other than the planned receiver(s). To play out the encryption and unscrambling the transmitter and receiver(s) should have coordinating encryption and decoding keys. A cunning method to produce these keys is to utilize the general population key circulation framework developed by Diffie and Hellman. That framework, in any case, concedes just a single combine of correspondence stations to share a specific match of encryption and decoding keys, people in general key dispersion framework is summed up to a gathering key conveyance framework (CKDS) which concedes any group of stations to have a similar encryption and unscrambling keys. • Q. Wu, Y. Mu, W. Susilo, B. Qin and J. Domingo-Ferrer, "Unbalanced Group Key Agreement," in Proc. Eurocrypt 2009, vol. LNCS 5479, Lecture Notes in Computer Science, pp. 153-170, 2009. A group key assention (GKA) convention enables an arrangement of clients to set up a typical mystery by means of open systems. Watching that a noteworthy objective of GKAs for most applications is to set up a classified channel among group individuals, we return to the group key assention definition and recognize the ordinary (symmetric) group key understanding from deviated group key assention (ASGKA) conventions. Rather than a typical mystery key, just a common encryption key is consulted in an ASGKA convention. This encryption key is open to assailants and compares to various decoding keys, every one of which is just processable by one group part. • Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and O. Farr`as, "Spanning Broadcast Encryption and Group Key Agreement," in Proc. Asiacrypt 2011, vol. LNCS 7073, Lecture Notes in Computer Science, pp. 143-160, 2011. Broadcast encryption (BE) plans enable a sender to safely broadcast to any subset of individuals however requires a trusted gathering to appropriate decoding keys. Group key assention (GKA) conventions empower a group of individuals to arrange a typical encryption key by means of open systems so just the individuals can unscramble the ciphertexts scrambled under the mutual encryption key, however a sender can't prohibit a specific part from decoding the ciphertexts. In this paper, we connect these two ideas with a half breed crude alluded to as contributory broadcast encryption (CBE). In this new crude, a group of individuals arrange a typical open encryption key while every part holds an unscrambling key. A sender seeing the general population group encryption key can restrict the unscrambling to a subset of individuals from his decision. Following this model, we propose a CBE plot with short ciphertexts. The plan is ended up being completely agreement safe under the choice n-Bilinear Diffie-Hellman Exponentiation (BDHE) supposition in the standard model. • D. H. Phan, D. Pointcheval and M. Strefler, "Decentralized Dynamic Broadcast Encryption," in Proc. SCN 2012, vol. LNCS, 2011. A broadcast encryption incorporates three substances: the group administrator managing enrollment, the encryptor encoding the information for enlisted customers as per a particular approach (the objective set), and the clients that unscramble the message on the off chance that they are approved. Open key broadcast encryption is fit for barring this one of a kind part of encryptor, by allowing a body to send scrambled information. We go above and beyond in the decentralization procedure, by evacuating the group supervisor, and in addition the expansion of further individuals to the framework, don't require any focal expert. Our development influences black-box to utilization of surely understood natives and can be considered as an expansion to the subset-cover structure.

III. Key Generation Technique

Key distribution sets (KDS) are used to generate key in which there are different types of combination of character are taken from end user at run time which is related to the document which user are going to share on the intended group with group key agreement.

Following are the few definitions of the KDS which giver complete idea about who the sets are form and key is generated by using the definitions.

Definition 1 = docid-S|!-docname-ddate-R|3419username

Definition 2 = ddate-username-R|4444-docnamedocid-S|%

Definition 3 = docname-S|$-username-R|7424-docidddate

docid:- which is the id of the document which is share among the group.

S|{!,%,$,@,#}:- S indicates the special symbol in which we have taken any symbol from the sets of the five symbol. docname :- is the name of the document at the time of sending taken given by the user.

ddate:- Date on which the document is going to share to the intended group.

R|3419:- R indicates the four digit random number generated by the system in which system can generate any number from 0000 to 9999 at randomly.

Username:- username of the sender which are going to share the document on a particular group or a single user which store their document on server for security purpose.

Random numbers are extremely useful, for example, in generating moves in a game or as test data for computer programs. If one is asked to "pick a number between one and a hundred", the task seems simple enough. But, if you need truly random numbers (each number is equally probable!), and if you want to generate them from a computer, the task is quite tricky as it turns out. Mathematicians have labored over this problem, and have devised robust techniques to generate random numbers. However, computers are deterministic (all actions are predictable at some level!), and, so, generating numbers that are "truly" random is not possible. However, we can get pretty close. Algorithms that generate random numbers, admittedly, provide "pseudorandom" numbers. But, for most purposes this is good enough.

Key generation working:

KDS generate for the every branch of the registered customer. It will select any one KDS set from the KDS set available using random algorithm. Random algorithms again select the any one algorithm from selected set of algorithm and generate key using that algorithm which generate session secrete key and Store session secrete key in Database in encrypted format.

Figure 1 Key generation working

Elliptic Curve Cryptography (ECC)

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create smaller, faster and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the multiplication of very large prime numbers.

The primary benefit promised by ECC is reducing storage, a smaller key size and transmission requirements, i.e. that an elliptic curve group could provide the same level of security Afforded by an RSA-based system with a large modulus and correspondingly larger key. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,

E - Elliptic Curve

P - Point on the curve

n -Maximum limit (This should be a prime number)

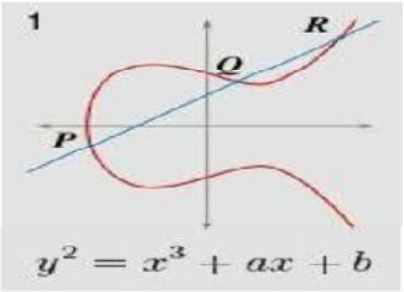

Figure 2 Simple elliptic curve

Key Generation

Key generation is an important part where user has to generate both public key and private key. The sender will be encrypting the message with receiver‘s public key and the receiver will decrypt its private key.

Now, user have to select a number ‗d‘ within the range of **‘n’**.

Using the following equation we can generate the

Public key Q = d * P

d = the random number that user have selected within the range of **(**1 to n-1**).**

P is the point on the curve. Q is the public key.

d is the private key.

Encryption:

Let ‗m‘ be the message that user are sending. user have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider ‘m’ has the point ‘M’ on the curve ‘E’. Randomly select ‗k‘ from [1 – (n-1)].Two cipher texts will be generated let it be C1 and C2**.**

C1 = k*P

C2 = M + k*Q

IV. Proposed Work

We present the Contributory Broadcast Encryption (ConBE) primitive, which is a hybrid of GKA and BE. This full paper provides complete security proofs, illustrates the necessity of the aggregatability of the underlying BE building block and shows the practicality of our ConBE scheme with experiments. First, we model the ConBE primitive and formalize its security definitions. ConBE incorporates the underlying ideas of GKA and BE. A group of members interact via open networks to negotiate a public encryption key while each member holds a different secret decryption key. Using the public encryption key, anyone can encrypt any message to any subset of the group members and only the intended receivers can decrypt. We formalize collusion resistance by defining an attacker who can fully control all the members outside the intended receivers but cannot extract useful information from the ciphertext. Second, we present the notion of aggregatable broadcast encryption (AggBE). Coarsely speaking, a BE scheme is aggregatable if its secure instances can be aggregated into a new secure instance of the BE scheme. Specifically, only the aggregated decryption keys of the same user are valid decryption keys corresponding to the aggregated public keys of the underlying BE instances. Finally, we construct an efficient ConBE scheme with our AggBE scheme as a building block. The ConBE construction is proven to be semi-adaptively secure under the decision BDHE assumption in the standard model.

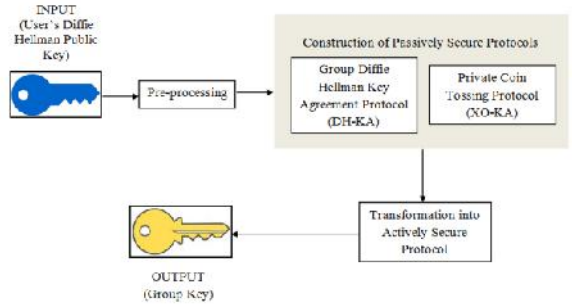

Fig. Proposed Architecture Diagram

V. Conclusion

Group key management is one of the basic building blocks in securing group communication. This method presented a Contributory Broadcast Encryption (ConBE) primitive, which is a hybrid of Group Key Agreement (GKA) and Broadcast Encryption (BE). A group of members interact via open networks to negotiate a public encryption key while each member holds a different secret decryption key. Using the public encryption key, anyone can encrypt any message to any subset of the group members and only the intended receivers can decrypt. Formalize 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. Broadcast Encryption scheme is aggregatable if its secure instances can be aggregated into a new secure instance of the BE scheme. Finally, this will created an efficient ConBE scheme with AggBE scheme as a building block.

Future Enhancement

Currently this project is implemented using Java and Eclipse over the LAN.

- It can be enhanced to work on the Mobile Ad-hoc Networks.

- Also it can be implemented Using NS-2 and can be used to measure the system performance.

- Instead of Encrypting Session Key using AES, DiffieHelman Key Exchange process can be incorporated.

References

[1]Y. Amir, Y. Kim, C. Nita-Rotaru, and G. Tsudik, "On the performance of group key agreement protocols," ACM Trans. Inf. Syst. Secur., vol. 7, no. 3, pp. 457–488, Aug. 2004.

[2] D. Augot, R. Bhaskar, V. Issarny, and D. Sacchetti, "An efficient group key agreement protocol for ad hoc networks," in Proc. 6th IEEE Int. Symp. World Wireless Mobile Multimedia Netw., 2005, pp. 576–580.

[3] A. Beimel and B. Chor, "Communication in key distribution schemes," in Proc. Adv. Cryptol., 1994, vol. 773, pp. 444–455.

[4] R. Blom, "An optimal class of symmetric key generation systems," in Proc. Adv. Cryptol., 1984, vol. 209, pp. 335–338.

[5] D. Boneh and M. K. Franklin, "An efficient public-key traitor tracing scheme," in Proc. Adv. Cryptol., 1999, vol. 1666, pp. 338–353.

[6] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in Proc. Adv. Cryptol ., 2005, vol. 3621, pp. 258–275.

[7] D. Boneh, A. Sahai, and B. Waters, "Fully collusion resistant traitor tracing with short ciphertexts and private keys," in Proc. 25th Int. Conf. Theory Appl. Cryptographic Tech., 2006, vol. 4004, pp. 573–592.

[8] D. Boneh and M. Naor, "Traitor tracing with constant size Cipher text," in Proc. 15th ACM Conf. Comput. Comm. Security, 2008, pp. 501–510.

[9] D. Boneh and A. Silverberg, "Applications of multilinear forms to cryptography," Contemporary Math., vol. 324, pp. 71–90, 2003.

[10] C. Blundo, L. A. Mattos, and D. R. Stinson, "Generalized Beimel- Chor schemes for broadcast encryption and interactive key distribution," Theor. Comp. Sci., vol. 200, no. 1–2, pp. 313–334, 1998.

Authors

NARSUNAIDU BORA is pursuing M.Tech in Sri Sivani College of engineering chilakapalem, Srikakulam, AP, India.

Dr. RAJENDRA KUMAR GANIYA did his Ph.D in Computer Science and Engineering from Andhra University in 2015, Visakhapatnam, received his M.Tech degree in Computer Science and Engineering from Acharya Nagarjuna University in 2005, Guntur, M.Sc degree in Computer Science from Andhra University in 2000 and B.Sc Computer Science from Andhra University in 1998, Visakhapatnam. He is working as Professor of Sri Sivani College of Engineering, Srikakulam and thorough professional with a vast experience of 17 years of service in the fields of Teaching, Research and Administration. His Research Interest includes Communication Networks, Cognitive Science, Nano Technology, Bio Medical and Human Computer Interaction.