A Unique Mechanism of Group Key Agreement for Contributory Broadcast Encryption

Z. Sowmya
CSE dept.G. Pulla Reddy engineering college
Kurnool, India

K. Ishthaq Ahamed
CSE dept. G. Pulla Reddy engineering college
Kurnool, India

Abstract: Encryption is used in a correspondence framework to secure data in the transmitted messages from sender to receiver. To execute the encryption in addition to decryption transmitter and receiver ought to have comparing encryption in addition to decryption keys. For transportation preventive measure data to group required broadcast encryption (BE). Broadcast Encryption sanctions a sender to securely broadcast to any subset of individuals and require a trusted gathering to disperse decryption keys. Group key agreement (GKA) primitive enable a group of members to obtain a common encryption key via open networks so that only the group members can decrypt the cipher texts encrypted under the shared encryption key, but a sender cannot exclude any particular member from decrypting the cipher texts. Here, we interface these two thoughts with a hybrid rough suggested as contributory broadcast encryption (ConBE). So, that group of members obtain common public encryption key while each member holds an unscrambling key. Going before this model, presenting a ConBE plotting of short figure works. We display the Contributory Broadcast Encryption (ConBE) demonstrate, which is amalgamation of GKA and BE. Social affair key declaration, contributory broadcast encryption, and provable security.

Keywords: Broadcast Encryption, Group key Agreement, and Contributory Broadcast Encry-ption.

I. INTRODUCTION

With the expansion in innovation progression in correspondence advances, there is an expan-ding interest of flexible cryptographic natives to secure group interchanges and calculation stages. These incipient platforms include instant-messaging implements, collaborative computing, mobile ad hoc networks and convivial networks. These new applications call for cryptographic natives enabling to users to safely encoding to any subset of the clients of the administrations without depending on a completely confided in merchant. Broadcast encryption (BE) is an all around considered crude planned for secure group-situated interchanges. It enables a sender to safely broadcast to any subset of group individuals. By the by, a BE framework intensely depends on a completely confided in key server who creates mystery decoding keys for the individuals and can read every one of the correspondences to any individuals. Group key agreement (GKA) is another surely knew cryptographic crude to anchor group-arranged correspondences. A traditional GKA enables a group of individuals to build up a typical mystery key by means of open systems. In any case, at whatever point a sender desires toward build an impression on a group, he must first join the group and run a GKA get-together to impart a secrecy key to estimated individuals all the more as of late, and to conquer this constraint, 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.

Be that as it may, neither traditional symmetric GKA nor the recently presented hilter kilter GKA enables the sender to singularly avoid a specific part from perusing the plaintext. Consequently, it is basic to discover more adaptable cryptographic natives permitting dynamic broadcasts without a completely tenable in merchant. This paper examines a nearby variety of the previously mentioned issue of one-round group key agreement conventions and spotlights "on the most proficient method to set up a secret channel without preparation for different gatherings in one round". We give a short outline of some new plans to understand this variety. Uneven GKA Observe that noteworthy objective of an GKAs for the most application is to be build up secret broadcast channel among the group. We examine the possibility to build up this direct in a trusted way as in the group individuals only arrange typical encryption key (open to assailants) yet hold particular mystery decoding keys. We present another class of GKA conventions which we name hilter kilter group key agreements understanding (ASGKAs), rather than the ordinary

GKAs. A particular arrangement is for every part to distribute an open key and withhold the separate mystery key, so the last ciphertext is worked as a connection of the hidden individual ones. Be that as it may, this unimportant arrangement is exceedingly wasteful: the ciphertext increments directly with the group measure; moreover, the sender needs to keep all the general population keys of the group individuals and independently scramble for every part.

We are occupied with nontrivial arrangements that don't experience the ill effects of these impediments. Group key agreement (GKA) is another surely knew cryptographic crude to anchor group-arranged correspondences. A traditional GKA enables a group of individuals to build up a typical mystery key by means of open systems. Notwithstanding, at whatever point a sender needs to make an impression on a group, he must be first to join the group and run GKA convention toward impart a mystery key to be expected individuals. All the more as of late presented deviated GKA in which just a typical group open key is arranged and each group part holds an alternate decoding key. Be that as it may, neither regular symmetric GKA nor the recently introduced awry GKA enable the sender to singularly prohibit a specific part from perusing the plaintext1. Consequently, it is fundamental to discover more adaptable cryptographic natives permitting dynamic broadcasts without a completely confided in merchant.

II. RELATED WORK

• In [5], they delineated to grasp a typical model where gathering controller (GC) issues the session keys fittingly. The favorable circumstances required for the GC to fitting session keys to assemble individuals intertwine correspondence, amassing and check assets. The correspondence ailment quality is normally assessed by the amount of information bits that should be transmitted from the GC to cluster individuals to pass on data of session keys. In this plan, data identified with session keys is encoded utilizing fumble controlling keys as opposed to encryptions. With everything considered, encoding and disentangling of a honest to goodness blunder control code have much (no shy of what one request) chop down check multifaceted nature than existing encryption and unscrambling figuring. In this way, estimation unpredictability of key scattering can be basically diminished. The practically identical idea of using bungle control codes to achieve security was used.

• In [2] they depicted that; this paper one will dodge these obstructions and shutting this opening by executing a novel key usage perspective. Despite this it can in like manner give web data safe. The customer can securely store their essential property or nostalgic assets. The propelled safe store box would then have the capacity to be appeared as an increase to a present electronic dealing with a record game plan. It furthermore uses a vpn security concern and procedure usage with a particular ultimate objective to give information securely to the proposed customer. Thusly, one can watch that the present key organization approaches don't give convincing responses for this issue. On one hand, GKAs gives a beneficial response for secure intergroup correspondence, anyway for a remote server, it requires the server to in the meantime stay online with the group individuals for various rounds of joint efforts.

• In [13] they illustrated, Remote pleasant social affairs using scrambled correspondence. Cases are found to gain power in GC correspondence developing in remote systems, versatile Ad-hoc arranges, vehicular specially appointed systems, et cetera. WMNs have turned into a simplicity approach to manage given fast Internet. A customary WMN is a multi bob different leveled remote framework. The player has quick wired Internet entry centers. The second level constitutes of work switches filling in as the multi-hop spine to connect with rest of clients and Internet through long far off fast remote strategies. The base layers fuse a far reaching number of portable framework customers. The end customers get to the framework either by a prompt remote association or through the chain of other partner customers prompting a near to work switches; by then the switch furthermore interfaces with remote customers through the remote spine and Internet. Security and assurance issues are of most outrageous concerning pushing it to the achievement of WMNs for their wide sending and for supporting organization orchestrated applications.

• In [9] portrayed that, In Emerging Technology Mobile adhoc Network (MANET) is for the most part used various zones, viably to achieve fast transmission and correspondence. In any case, it can't achieve fast transmission/broadcasting in Remote Area. To beat this issue new key organization worldview strategy is used. In this proposed system the new key organization worldview outlines some social affair. In that social occasion select any of the center point/structure in light of that need to send the secret key scattering among sender and recipient to upgrade snappy data transmission in remote Area. Each and every data transmission, secret key will be made and besides should be revived. In that remote area software engineers should theft the data, so give protection against the unapproved person. Using key reviving technique transmit the data brisk, strong and more securable way. To make Cooperative social events using another Key organization worldview in Remote Area. The Computation overhead and Communication Cost are free of social event estimate. Using rekeying systems beneficial way to deal with achieves any number of expansion/eradication procedures will be done and strong security against the crash in that remote Area.

III. MODELING CONTRIBUTORY BROADCAST ENCRYPTION

We start by formalizing the ConBE thought crossing over the GKA and BE natives. In ConBE, a group of individuals first mutually build up an open encryption key; at that point a sender can uninhibitedly choose which subset of the group individuals can unscramble the ciphertext. Since the arranged open key is normally utilized to transmit session keys, we characterize a ConBE plot as a key encapsulation mechanism (KEM).

A. Syntax

We initially characterize the algorithms that form a ConBE plot. Give 2 N a chance to mean the security parameter. Assume that a group of individuals {U_1,...,Un} need to mutually build up a ConBE framework, where n is a positive whole number and every part U_i is recorded by i for $1 \leq i \leq n$. To center on ConBE, we expect that the correspondences between individuals are confirmed. Be that as it may, we don't accept any classified channel amid the execution of the convention. Formally, a ConBE conspire (ParaGen; CBSetup; CBEncrypt; CBDecrypt) comprises of the accompanying four polynomial-time algorithms.

ParaGen ($1^{ƛ}$). This algorithm is utilized to produce worldwide parameters. It takes as information a security parameter and it yields the framework parameters, including the group measure n.

CBSetup ($U_1(x_1)$,....,Un(x_n)). This intelligent algorithm is mutually kept running by individuals U_1,...,Un to set up a BE plot. Every part U_i takes private input x_i (and her/his arbitrary coins speaking to the part's irregular internal state data). The interchanges between individuals adhere to confirmed and open procedures. The algorithm will either prematurely end or effectively end. In the event that it ends effectively, every client U_i yields a decoding key dk_i safely kept by the client and a typical group encryption key gek shared by all the group individuals. The group encryption gek is freely open. On the off chance that the algorithm prematurely ends, it yields NULL. Here, we leave the information framework parameters understood. We signify this procedure by ($U_1(dk_1)$,....,Un(dk_n); gek) CBSetup($U_1(x_1)$, , $U_n(x_n)$). CBEncrypt(S, gek). This group encryption algorithm is controlled by a sender who is expected to know general society group encryption key. The sender might possibly be a group part. The algorithm takes as sources of info a beneficiary set S{1,...,n} and people in general group encryption key gek, and it yields a couple (c,ξ), where c is the ciphertext and is the mystery session key in a key space K. At that point (c; S) is sent to the beneficiaries.

CBDecrypt(S,j,dkj,c). This decoding algorithm is controlled by each planned beneficiary jϵS. It takes as information sources the beneficiary set S, record j, the collector's decoding key dkj, and a ciphertext c, and it yields the mystery session key. A ConBE conspire is right if the individuals in the beneficiary set can simply accurately unscramble when the individuals and the sender take after the plan sincerely. Formally, it is characterized as takes after.

Definition 1 (Correctness). A ConBE conspire is said to be right if for any parameter ƛϵN and any component in the session key space, ($U_1(dk_1)$,...,Un(dkn); gek)

←CBSetup($U_1(x_1)$,...,Un(x_n)), and (c,ξ) ←CBEncrypt (S,gek), it holds that CBDecrypt(S, j, dkj , c) = for any j ϵ S.

B. Security Definitions

We next characterize the security of a ConBE conspire. A few techniques have been proposed to change public key encryption (PKE) with security against picked plaintext assaults (CPA) into encryption against adaptively picked ciphertext assaults (CCA2) in the standard model. In [48], Canetti et al. recommended change from CPA secure IBE to CCA2-secure PKE utilizing a one-time signature. In [49], Matsuda and Hanaoka proposed to acquire CCA2-secure PKE from any CPA-secure PKE with a general computational extractor. In [50], Liu et al. acquired CCA2-secure ABE from CPA-secure ABE without additional cryptographic natives, however with an extra on-the-fly sham trait. We take note of that these techniques are appropriate to our ConBE setting with/without adjustment (e.g., by including a the-fly sham recipient). The cost relies upon the techniques, i.e., an all inclusive computational extractor, a one-time signature or a spurious client. Thus, it is adequate to just characterize the CPA security of a ConBE conspire. Nonetheless, taking note of that ConBE is intended for circulated applications where the clients are probably going to be defiled; we incorporate full intrigue obstruction into our security definition.

The completely plot safe security of a ConBE conspire is characterized by the accompanying security amusement between a challenger CH and an assailant A.

Instatement: The challenger CH runs ParaGen with a security parameter and gets the framework parameters. The framework parameters are given to the aggressor A.

Questions: Attacker A can influence the accompanying queries to challenger CH.

Execute. An utilizations the personalities of n individuals U_1,...U_n to inquiry CH. The challenger runs CBSetup ($U_1(x_1)$,....,Un(x_n)) for the benefit of the n individuals, and reacts with the group encryption key gek and the transcripts of CBSetup to A.

Degenerate: A sends i to the Corrupt prophet kept up by CH, where i ϵ{1,....,n}. The challenger CH restores the private information and inward arbitrary coins of U_i amid the execution of CBSetup. Uncover A sends I to the Reveal prophet kept up by CH, where iϵ{1,...,n}. The challenger CH reacts with The Corrupt prophet is utilized to demonstrate an aggressor who bargains a few individuals amid the set-up stage to establish the group encryption key. The Reveal prophet is utilized to catch the decoding key spillage after the ConBE framework has been built up. This distinction can be utilized to separate the security against assaults amid the set-up arrange from the security against assaults after a ConBE framework is sent.

We expect that the correspondence channels between members are confirmed amid the CBSetup stage to set up group encryption key. This is to enable every client to approve that they got convention transcripts are from legitimate individuals. The most normal approach to set up confirmed channels is through an open key framework (PKI): every client enlists an open key to an accreditation specialist CA and utilizations the comparing private key to sign any message she produces amid the CBSetup arrange. Subsequently, the legitimacy of the CBSetup transcript from a client can be checked by every other client. Note that after this stage has been finished and the group encryption key gek has been settled upon, messages scrambled under this group key can't be comprehended by CA, on the grounds that the last does not know the comparing decoding keys. For example, in an informal organization application, the interpersonal organization administrator can fill in as the CA and confirm the clients' open keys used to verify correspondence. Thusly, the administrator is just in part trusted and can't decode the encoded messages along these lines shared among the clients under gek.

Based on aggregatable BE scheme, we implement a ConBE scheme through short ciphertexts. Assume that the group size is by most n. Let ϒ= (p,G,GT , e)← PairGen(1ʎ), and g, h1, . . . ; hn be independent generators of G. The system parameters are Π=(ʎ, n,ϒ g, h1, . . . , hn).

Setup: The set-up of a ConBE system consists of the following
three procedures:

_ GroupKeyAgreement: For 1 ≤ k ≤n, member k does the following:

- Randomly choose $X_{i,k} \in \mathbb{G}, r_{i,k} \in \mathbb{Z}_p^*$;
- Compute $R_{i,k} = g^{-r_{i,k}}, A_{i,k} = e(X_{i,k}, g)$;
- Set $PK_k = ((R_{0,k}, A_{0,k}), \ldots, (R_{n,k}, A_{n,k}))$;
- For $j = 1, \ldots, n,\ j \neq k$, compute $\sigma_{i,j,k} = X_{i,k} h_j^{r_{i,k}}$ for $i = 0, \ldots, n$, with $i \neq j$;
- Set $d_{j,k} = (\sigma_{0,j,k}, \ldots, \sigma_{j-1,j,k}, \sigma_{j+1,j,k}, \ldots, \sigma_{n,j,k})$;
- Publish $(PK_k, d_{1,k}, \ldots, d_{k-1,k}, d_{k+1,k}, \ldots, d_{n,k})$;
- Compute $d_{k,k}$ accordingly and keep it secret.

GroupEncryptionKeyDerivation: The group encryption key is

$$PK = PK_0 \circledast \cdots \circledast$$

$$PK_n = ((R_0, A_0), \ldots, (R_n, A_n))$$

where $R_i = \prod_{k=1}^{n} R_{i,k}$, $A_i = \prod_{k=1}^{n} A_{i,k}$ for $i = 0, \ldots, n$.

- MemberDecryptionKeyDerivation : For 0 ≤ i ≤ n, 1 ≤ j ≤ n and i≠ j, member j can compute her decryption key

$$d_j = (\sigma_{0,j}, \ldots, \sigma_{j-1,j}, \sigma_{j+1,j}, \ldots, \sigma_{n,j})$$

where

$$\sigma_{i,j} = \sigma_{i,j,j} \prod_{k=1, k\neq j}^{n} \sigma_{i,j,k} = \prod_{k=1}^{n} \sigma_{i,j,k} = \prod_{k=1}^{n} X_{i,k} h_j^{r_{i,k}}.$$

CBEncrypt: Assume that a sender (not necessarily a Group member) wants to send to receivers in S ≤ {1, . . . , n}
a session key ϵ. Set S ={0, 1, . . . , n} \ S. Randomly pick t in
Zp* and compute the ciphertext c =(c1, c2) where

$$c_1 = g^t, c_2 = \left(\prod_{i \in \overline{\mathbb{S}}} R_i\right)^t.$$

Output (c, ξ) where $\xi = (\prod_{i \in \overline{\mathbb{S}}} A_i)^t$.
Send $(\mathbb{S}, c)$ to the receivers.

- CBDecrypt: If j ϵ S, receiver j can extract ϵ from the ciphertext c with decryption key dj by computing

$$e\left(\prod_{i \in \overline{\mathbb{S}}} \sigma_{i,j}, c_1\right) e(h_j, c_2) = \xi.$$

- The correctness of the system directly follow from the fact that under-lying BE scheme is to correct and key-homo- morphic. As to security, we have following theorem, whose proof is given in Section 6.2.

IV. PERFORMANCE ANALYSIS

A. Theoretical Analysis

We initially look at the online unpredictability that is basic for the reasonableness of a ConBE conspires. While assessing the execution, we utilize the generally embraced measurements for customary BE plans. In these measurements, the expenses of straightforward tasks (e.g., read the files of recipients and play out some basic evaluation of group components related to these lists) and correspondence (e.g., the paired portrayal of the collectors' set) are not thought about. After the CBSetup technique, a sender needs to recover and store the group open key PK comprising of n components in G and n components in G_T. In addition, for encryption, the sender needs just two exponentiations and the ciphertext simply contains two components in G. This is about n times more effective than the paltry arrangement. At the collector's side, notwithstanding the depiction of the bilinear combine which might be shared by numerous other security applications, a recipient needs to store n components in G for decoding. For decoding, a recipient needs to figure two single-base bilinear pairings (or one two base bilinear matching). The online expenses on the sides of both the sender and the collectors are extremely low.

We next talk about the unpredictability of the CBSetup methodology to set up a ConBE framework. The overhead caused by this technique is O (n^2). This method should be run just once and this should be possible disconnected before the online transmission of mystery session keys. For example, in the interpersonal organizations case, various companions trade their CBSetup transcripts and build up a ConBE framework to anchor their resulting sharing of private picture/videos. Since ConBE permits renouncing persons, the persons don't have to reassemble for another kept running of the CBSetup technique until the point when some new companions join. From our own understanding, the group lifetime for the most part keeps going from weeks to months. These perceptions infer that our convention is commonsense in reality. Besides, if the underlying group is too extensive, an effective exchange off can be utilized to adjust the on the web and disconnected expenses. Assume that n is a shape, i.e., n = $n_1{}^{3}$, and the underlying group has n individuals. We separate the full group into $n_1{}^{2}$ subgroups, every one of which has n1 individuals. By applying our essential ConBE to every subgroup, we get a ConBE plot with O (n_1^2)-measure transcripts per part amid the disconnected phase of group key foundation; a sender needs to do O (n_1^2) encryption tasks of the fundamental ConBE conspire, which produces O (n_1^2)- estimate cipher texts. Thusly, we acquire a semi-versatile ConBE conspire with O ($n^{2/3}$) many-sided quality. This is practically identical to forward open key BE frameworks whose intricacy is O ($n^{1/2}$).

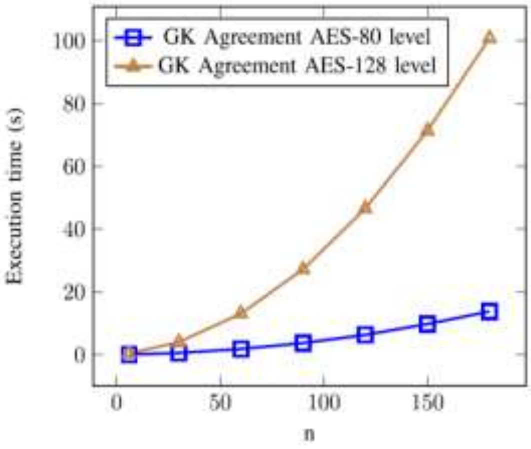

Fig 1

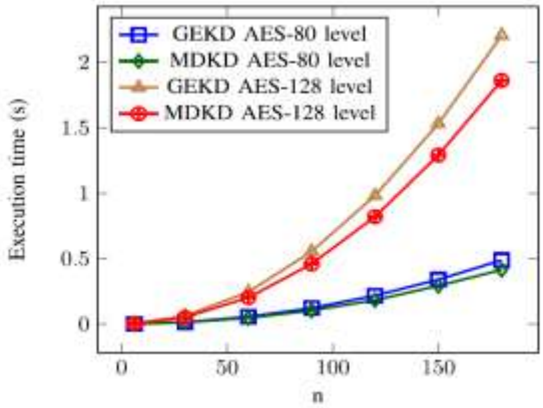

Fig 2

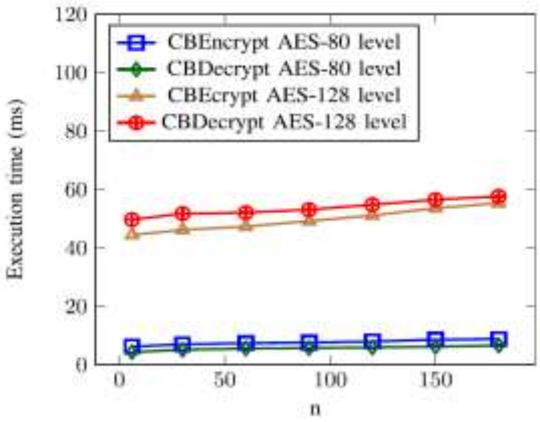

Fig 3

Fig.1,2,3. Execution time of Group Key Agreement, Group Encryption Key Derivation, Member Decryption Key Derivation, CB Encrypt, and CBDecrypt for AES-80 and AES-128 levels

B. Experimental Analysis

In this segment we exhibit test comes about on our ConBE plot. The tests were kept running on a PC with Intel Core i7-2600 CPU at 3.4GHz, utilizing the C programming dialect. The cryptographic tasks were executed utilizing the Pairing-Based Cryptography library2. Following the NIST-2012 key size recommendation3, we understood our convention for a direct AES-80 level and a more regular AES-128 level, comparing to the security level of a perfect symmetric figure with 80-bit and 128-piece mystery keys, individually. We utilized Type A pairings developed on the bend $y^2 = x^3 + x$ with inserting degree 2. As needs be, in the main case for AES-80 level, G has 512-piece components of a 160-piece prime request and G_T has 1024-piece/128-byte components; and in the second case for AES-128 level, G has 1536-piece components of a 256-piece prime request and GT has 3072-piece/386-byte components, individually. We performed investigates the disconnected methods including Group Key Agreement, Group Encryption Key Derivation and Member Decryption Key Derivation, and the online techniques including CBEncrypt and CBDecrypt for various group sizes n = 6, 30, 60, 90, 120, 150, 180. The qualities for CBEncrypt and CBDecrypt think about the most pessimistic scenario, i.e., |S| = 1. Likewise, we didn't advance the hidden blending related parameters or tasks, e.g., by picking a substantial prime normal for the base field and the prime request p with most bits 0 (or 1), and by quickening multi-base exponentiations/multi-base pairings. Consequently, the down to earth execution of our convention can be superior to the delineated test comes about.

In Fig.1, the security level of our convention is estimated by the mystery key size of AES (thought to be a perfect symmetric figure), i.e., AES with a truncated 80-bit key and AES with a standard 128-piece key. The furthest left diagram in the figure shows the group key agreement time for various group sizes and diverse security levels. The execution time develops quadratically with the group measure, and furthermore develops with the security level. This is steady with our hypothetical examination, in light of the fact that the pairings and the exponentiations overwhelm the calculation costs. To accomplish a direct 128-piece security, the execution time is around 3 minutes for a group of 180 clients. This is practical as the GKA method just should be run once and after that one can broadcast to any subset of the clients, without re-running the convention or any additional denial sub convention. The focal diagram in Fig.1 demonstrates an opportunity to separate the group encryption key and the decoding key for various group sizes and distinctive security levels. Additionally to the group key agreement time, the key extraction time likewise develops with the security level and the group estimate. In any case, even in the most pessimistic scenario, just around 3 seconds are required, which is moderate practically speaking.

The furthest right diagram in Fig.1 outlines the online session key encryption/decoding time. It can be seen that the time is relatively steady for various group sizes, which is predictable with the hypothetical examination. Both the session key encryption and decoding take under 10ms for a 80-bit security level, and under 80ms for a 128-piece security level. After the framework is set up, the session key transmission is extremely effective, which is easy to understand and certainly influences our ConBE to plot practical. We likewise performed probes cost tradeoff between set-up and online encryption. For n = 180 and AES-128 level, the execution times for Group Key Agreement, Group Encryption Key Derivation, Member Decryption Key Derivation, CBEncrypt and CBDecrypt are 101s, 2.20s, 1.86s, 55.3ms, and 57.6ms, individually. Be that as it may, utilizing the exchange off depicted in the past area, particularly taking subgroups of 6 clients, the circumstances end up 410ms, 2.05ms, 1.63ms, 1.33s, and 57.6ms. The setup effectiveness was fundamentally enhanced, at the cost of a 1.33s encryption time, to be contrasted with a 55.3ms encryption time without tradeoff.

V. CONCLUSION

In this paper, we formalized the ConBE crude. In ConBE, anyone can send puzzle messages to any subset of the social affair people, and the structure does not require a confided in key server. Neither the difference in the sender nor the dynamic choice of the arranged recipients requires extra adjusts to organize bundle encryption/unscrambling keys. Taking after the ConBE show, we instantiated and gainful ConBE arrange for that is secure in the standard model. As adaptable cryptographic crude, our novel ConBE thought opens another street to set up secure broadcast stations and can be depended upon to anchor different creating coursed computation applications.

REFERENCE

[1] Ankush V. Ajmire, Prof. Avinash P. Wadhe,‖Review paper on Key Generation Technique With Contributory Broadcast Encryption, ‖ IC-QUEST 2016, 5Th International Conference on Quality Up-gradation in Engineering, Science & Technology on 12th April 2016.

[2] C.K. Wong, M. Gouda and S. Lam, Secure Group Communications Using Key Graphs,‖ IEEE/ACM Transactions on Networking, vol. 8, no. 1, pp. 16-30, 2000

[3] J.H. Park, H.J. Kim, M.H. Sung and D.H. Lee, Public Key Broadcast Encryption Schemes With Shorter Transmissions,‖ IEEE Transactions on Broadcasting, vol. 54, no. 3, pp. 401-411, 2008.

[4] Z. Yu and Y. Guan, A Key Management Scheme Using Deployment Knowledge for Wireless Sensor Networks,‖ IEEE Transactions Parallel Distributed Systems, vol. 19, no. 10, pp. 1411-1425, 2008.

[5] Q. Wu, B. Qin, L. Zhang, J. Domingo, Contributory Broadcast Encryption with Efficient Encryption and Short Ciphertexts,‖ IEEE Transactions On Computer, 2015.

[6] 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.

[7] Q. Wu, Y. Mu, W. Susilo, B. Qin and J. Domingo-Ferrer, Asymmetric Group Key Agreement,‖ in Proc. Eurocrypt 2009, 2009, vol. LNCS 5479, Lecture Notes in Computer Science, pp. 153-170.

[8] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and O. Farras, Bridging Broadcast Encryption and Group Key Agreement,‖ in Proc. Asiacrypt2011, 2011, vol. LNCS 7073, Lecture Notes in Computer Science, pp. 143-160.

[9] D. H. Phan, D. Pointcheval and M. Strefler, Decentralized Dynamic Broadcast Encryption,‖ in

Proc. SCN 2012, 2011, vol. LNCS 7485, Lecture Notes in Computer Science, pp. 166-183.

[10] M. Steiner, G. Tsudik and M. Waidner, Key Agreement in Dynamic Peer Groups,‖ IEEE Transactions on Parallel and Distributed Systems, vol. 11, no. 8, pp. 769-780, 2000.

[11] A. Sherman and D. McGrew, ―Key Establishment in Large Dynamic Groups Using One-way Function Trees,‖ IEEE Transactions on Software Engineering, vol. 29, no. 5, pp. 444- 458, 2003.

[12] Y. Kim, A. Perrig and G. Tsudik, ―Tree-Based Group Key Agreement,‖ ACM Transactions on Information System Security, vol. 7, no. 1, pp. 60-96, 2004.

[13] Y. Mao, Y. Sun, M. Wu and K.J.R. Liu, ―JET: Dynamic Join Exit- Tree Amortization and Scheduling for Contributory Key Management,‖ IEEE/ACM Transactions on Networking, vol. 14, no. 5, pp. 1128-1140, 2006.

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