Auxiliary Propagate Encoding with Efficient Encryption and Short Ciphertext

[1]Prof. Prerna Kulkarni, [2]Aditya G. Tiwari, [3]Santosh V. Sony, [4]Sriram M. Torvi

[1]Asst. Professor, [2,3,4]UG Student, [1,2,3,4]Computer Engg. Dept. Shivajirao S.Jondhle College of Engineering & Technology, Asangaon, Maharshatra, India.

[2]*tiwariaditya1995@gmail.com*, [3]*santoshsony678@gmail.com*, [4]*sriram.torvi@gmail.com*

Abstract—Conventionally broadcast encryption (BE) schemes enable a sender to securely propagate to certain members of group, although it needs a trusted party to interchange decoded passkeys. Group key agreement protocols enables a group of members to setup a common encryption passkey through spread out networks so that only the batch members can decode the ciphertextsviz encrypted under the shared encryption key, but a sender cannot debar any particular member from decrypting the cipher texts. This paper infers two notions with a hybrid primitive referred to as Auxiliary Propagate encoding. In this new primitive, a common public encoding key is agreed by group members who hold a individual decoding passkey. A sender viewing the public group encoding passkey can restrict the decoding to a subdivision of members of his preference. Exponentiation presumption in the standard imitation. Of unaided concern, the paper presents a new BE scheme that is aggregately. The cumulative property is shown to be to construct cutting-edge protocols.

Keywords—Multicast encoding, Auxiliary Propagate Encoding, Provable Security, Group key agreement.

I. INTRODUCTION

Along the rapidly leading and prevalent communion technologies, there is an increasing bid for handy cryptographic primeval to protect group conversations and ciphering platforms. These platforms include instant-messaging tools, collaborative ciphering, mobile ad hoc networks and communal net [5]. These new applications call for cryptographic primitives allowing a sender to soundly encrypt to any subdivision of the users of the services without relying on a fully credible dealer. Broadcast encoding is a well-studied primeval intended for secure group-oriented communications [1]. It allows a sender to soundly broadcast to any subdivision of the group members.

Nonetheless, a BE system heavily relies on a fully trusted key server who produces classified decoding passkeys for the members and can read all the communion to any members. Group key agreement is another well-defined cryptographic primeval to secure group-oriented communions. A traditional GKA enables a group of members to setup a common secret passkey through spread out networks. Although, whenever a sender wants to exchange an information to a group, he must first add the group and run a GKA protocol to share a restricted passkey with the expected members. More recently, and to overcome this limitation, Wu et al. popularized asymmetric GKA, a common public encoding key is agreed by group members who hold a individual decoding passkey. Although, neither newly presented asymmetric GKA nor the conventional symmetric GKA allows the sender to freely exclude any certain member from analyzing the plaintext. Hence, it is necessary to find several adjustable cryptographic primeval enabling dynamic broadcasts without a fully credible dealer [4].

The Auxiliary Propagate Encoding primitive, viz a hybrid of GKA and BE. Compared to its preliminary Asia crypt 2011 version, it provides complete security proofs, elaborates the necessity of the aggregability of the hidden BE building block and shows the pragmatism of the scheme with tryouts. The main contributions are as follows. First, the primitive and explains its security definitions. Auxiliary Broadcast Encoding incorporates the elemental ideas of GKA and BE. A group of members interact through free networks to agree a public encoding passkey while each member holds a different secret decoding key. Using the public encryption passkey, anyone can encode any message to any subdivision of the group members and only the intended receivers can decrypt.

Unlike GKA, Auxiliary entitles the sender to prohibit some members from reading the ciphertexts. Compared to Broadcast Encryption, Auxiliary Propagate Encoding does not need a fully credible third party to set up the system. Characterize collusion resistance by defining an attacker who can fully control every member farther the affianced receivers but cannot extract useful message from the cipher text.

Second, the notion of aggregable broadcast encoding. Contemptuously speaking, a Broadcast Encoding scheme is

aggregable if its secure instances can be aggregated into a new secure instance of the BE system. Specifically, only the aggregated decoding keys of the same user are valid decoding keys corresponding to the aggregated public passkeys of the hidden Broadcast Encryption examples. The aggregability of AggBE schemes is beneficial in the manufacturing of scheme and the BE schemes in the literature are not aggregable. A detailed AggBE system tightly proven to be fully collusion-resistant beneath the decision BDHE assumption. The projected AggBE system offers effectual encoding/decoding and short ciphertexts.

Certainly, create an effectual Auxiliary Broadcast Encoding scheme with AggBE scheme as a building block.. Only one round is needed to form the public group encoding passkey and set up the Auxiliary Broadcast Encoding system. After the system set-up, the storage cost would be O(n) for sender as well as for group members, where n is the number of group members taking part in the setup stage. Although, the online complexity (which dominates the practicality of a Auxiliary Broadcast Encoding scheme) is very low. Post trade-off, the variant has O(n2=3) complexity in communion, calculations and storage. This is comparable to up-to-date regular Broadcast Encoding schemes which have O(n1=2) complexity in the same performance metrics, but system does not require a credile passkey dealer. Execute a chain of experiments and the experimental results verify the practicality of scheme.

A. Potential Application

A potential application of Auxiliary Propagate Encoding is to secure data exchanged among friends via social networks. Since the Prism scandal, people are desperately concerned about the privacy of their personal data shared with their friends over social networks. Auxiliary Propagate Encoding can provide a feasible solution to this problem. Indeed, Phan et al underlined the applications of Auxiliary Propagate Encoding to social networks. In this scenario, if a group of users want to share their data without letting the social network operator know it, they this Encoding scheme. Since the setup procedure of Encoding only requires one round of communication, each member of the group just needs to broadcast one message to other intended members in a send-and-leave way, without the synchronization requirement. After receiving the messages from the other members, all the members share the encryption key that allows any user to selectively share his/her data to any subgroup of the members. Furthermore, it also allows sensitive data to be shared among different groups. Other applications may include contemporary messaging among family members, protected scientific research tasks jointly conducted by scientists from different places, and disaster rescue using a mobile ad hoc network [7]. A common feature of these scenarios is that a group of users would like to exchange sensitive data but a fully credible third party is unavailable. Encoder provides an efficient solution to these applications.

II. LITERATURE SURVEY

A. Paper on Broadcast Encryption

Several schemes that enable a center to broadcast a secret to any subset of authorized users out of a universe of size nso that coalitions of k users not in the privileged set cannot learn the secret. The most interesting scheme requires every user to store O(k log k Several schemes that allow a center to broadcast a secret to log n)keys and the center to broadcast O(k2 log2 k log n) messages regardless of the size of the privileged set [1]. This scheme needs every user to store O(log k log(1/p)) keys and the center to broadcast O(k log2 k log(1/p)) messages.

B. Paper on Collusion Resistant Broadcast Encryption With Short Ciphertexts and Private Keys

This system describe two new public key broadcast encryption systems for stateless receivers. Both systems are fully secure against any number of colluders. This construction both ciphertexts and private keys are of constant size (only two group elements), for any subset of receivers. The public passkey size in this system is linear in the total number of receivers. Second system is a generalization of the first that yields a trade-off between ciphertext size and public passkey size. The system achieves a collusion resistant broadcast system for n users where both ciphertexts and public passkeys are of size O(√n) for any subset of receivers [4].

C. Paper on A Conference Key Distribution System

Encryption is used in a communication system to safeguard information in the transmitted messages from anyone other than the intended receiver [2]. To perform the encryption and decryption the transmitter and receiver ought to have matching encryption and decryption keys. A wise way to generate these keys is to use the public passkey distribution system invented by Diffie and Hellman. The public key distribution system is generalized to a conference passkey.

III. PROPOSED SYSTEM

The Auxiliary Propagate Encoding primitive, provides complete security proofs, A group of members interact through free networks to agree a public encoding passkey while each member holds a different secret decoding key. Using the public encryption passkey, anyone can encode any message to any subdivision of the group members and only the intended receivers can decrypt. It uses AES for encoding, this encrypted data is stored on the server, only the data owner/admin can give access to these files to the end-user. End-user without the privileges to access shall be marked as invalid user. Member or owner from one group doesn't have liberty over another group's data.

Table-2.1 comparative Study.

SR NO	Paper Title And Methods	Author's Name	Merits	Demerits	Problem	Solution	Future Work
1.	Broadcast Encryption (Symmetric Encryptions, Secret key Distributions & management)	A. Fiat and M. Naor	Provides secure group-oriented communications	Existing GKA protocols cannot handle sender/member changes efficiently	Requires a trusted third party to distribute the keys.	Using Asymmetric group key agreement (ASGKA) to overcome this.	Future work will concern the implementation of the ASGKA scheme to incorporate the following.
2.	Collusion Resistant Broadcast Encryption with short Ciphertext and private keys	Dan Boneh , Craig Gentry	Provides a collusion resistant system.	Cannot handle large sets of groups.	Collusion resistant is limited to a relatively small group.	Using appropriate parametrization	Future works will concern the reduction of collusion by constructing both Ciphertext and private key of constant size.
3.	A Conference Key Distribution System (Security in digital systems ,Conference key distribution)	I. Ingemarsson, D.T. Tang and C.K. Wong	Provides a system using That distributes key using contributory key generation.	It is immune to insecurities due to symmetric functions of degree two.	As the key was a symmetric function of degree two, it was insecure.	Using a asymmetric function instead of symmetric function.	Future research will be devoted to methods that can use asymmetric function for higher security.
4.	Key Agreement in Dynamic Peer Groups (Multi-party Computation)	Michael Steiner,	Can handle system with constantly changing members and senders.	It is not efficient for relatedly large set of groups.	Works only for relatively small and non-hierarchical groups.	Using key transport mechanism.	Future research Will including the methods adopted in this.
5.	Broadcast Encryption (Symmetric Encryptions, Secret key Distributions & management)	A. Fiat and M. Naor	Provides secure group-oriented communications	It requires a fully trusted third party and direct link	It is more expensive as direct link has to be established	Cost can be minimised using Contributory key generation schemes or using Conbe Scheme.	Future research will be including plans to implement the schemes to cut down expenses.
6.	Contributory Broadcast Encryption With Efficient Encryption and Short Ciphertexts	Qianhong ,Bo Qin, Lei Zhang,Josep Domingo-Ferrer	Doesn't require trusted third Party to set up the system.	As it is more flexible , it compromises on some set of performances.	Cannot handle changes in server/member efficiently	Using auxiliary group Encoding	

IV. ALGORITHMS

A. AES algorithm

1. KeyExpansions - round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round

1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. AddRoundKey

4. Final Round (no MixColumns)

1. SubBytes
2. ShiftRows
3. AddRoundKey.

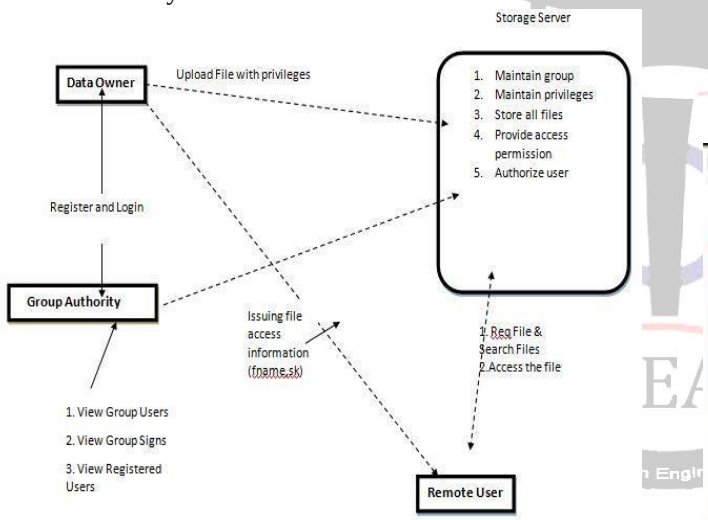

Fig. 1 Proposed System

B. SHA1 Algorithm:

1 For loop on k = 1 to N
(W(0),W(1),...,W(15)) =
M[k]

2 For t = 16 to 79 do:

W(t) = (W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16)) <<< 1

3 A = H0, B = H1, C = H2, D = H3, E = H4

4 For t = 0 to 79 do:

TEMP = A<<<5 + f(t;B,C,D) + E + W(t) + K(t) E = D, D = C, C = B<<<30, B = A, A = TEMP
End of for loop

5 H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E

V. MATHEMATICAL MODEL

Group Key Agreement. For 1 ≤k ≤n, member k does the following:

– Randomly choose Xi,k ϵG, ri,k ϵZp̌;
– Compute Ri,k = g-ri,k, Ai,k = e(Xi,k, g);
– Set PKk = ((R0,k , A0,k),….,(Rn,k, An,k));
– For j = 1, ……., n , j ≠ k, compute σi, j ,k= Xi,khj^{ri,k}for i = 0,……,n, with i ≠j;
– Set dj,k = (σ0,j,k,….., σj-1,j,k,σj+1,j,k,……,σn,j;k);
– Publish (PKk, d1,k, ……,dk-1;k, dk+1,k,……., dn,k);
– Compute dk,k accordingly and keep it secret.

- Group Encryption Key Derivation.The group encryption key is

PK = PK0 PKn = ((R0, A0), ……, (Rn, An))

where Ri =Π^{n}k= 1Ri,k, Ai =Π^{n}k=1Ai,kfor i = 0,……,n.

The group encryption key PK is publicly computable.
• Member Decryption Key Derivation: For 1 ≤i≤ n 1 ≤j≤ n and i ≠ j, member j can compute her decryption key

dj = (σ 0,j, ….., σ j-1,j,σj+1,j,……,σn,j)
where

$$\sigma_{i,j} = \sigma_{i,j,j} \prod_{k=1,k\neq 1}^{n} \sigma_{i,j,k} = \prod_{k=1}^{n} \sigma_{i,j,k} = \prod_{k=1}^{n} X_{i,k} h^{r}_{j}$$

VI. DESIGN DETAILS

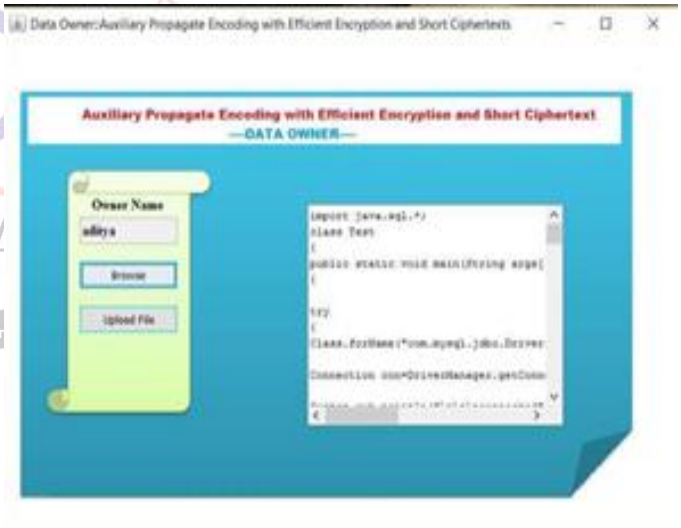

Fig no 1: Snapshot-Owner Uploading

Fig no 2: Snapshot-User Downloading the file

VII. CONCLUSION

We have tried to implement the paper "Qianhong Wu, , Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Oriol Farr`as, and Jes´us A. Manj´on", "Contributory Broadcast With Efficient Encryption and Short Ciphertext", IEEE Transactions of computer, February 2016 and according to the implementation the conclusion is that in AggBE a data owner can upload and save the data on the server in an encrypted form, and the system does not require a trusted key server. If the End-user wishes to gain access of the file, prior permission and privileges shall be required, without which the services would be denied. Neither the change of the sender nor the dynamic choice of the intended receivers require extra rounds to negotiate group encryption/decryption keys. Following the AggBE model, it instantiated an efficient AggBE scheme that is secure in the standard model. As a versatile cryptographic primitive, novel AggBE notion opens a new avenue to establish secure broadcast channels and can be expected to secure numerous emerging distributed computation applications.

REFERENCES

[1] A. Fiat and M. Naor, "Broadcast Encryption," in Proc. Crypto 1993, 1993, vol. LNCS 773, Lecture Notes in Computer Science, pp. 480- 491.

[2] 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.

[3] 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.

[4] http://en.wikipedia.org/wiki/PRISM %28surveillance program%29, 2014.

[5] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and O. Farr`as, "Bridging Broadcast Encryption and Group Key Agreement," in Proc. Asiacrypt 2011, 2011, vol. LNCS 7073, Lecture Notes in Computer Science, pp. 143-160.

[6] 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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] C. Boyd and J.M. Gonz´alez-Nieto, "Round-Optimal Contributory Conference Key Agreement," in Proc. PKC 2003, 2003, vol. LNCS 2567, Lecture Notes in Computer Science, pp. 161-174.

[12] W.-G. Tzeng and Z.-J. Tzeng, "Round Efficient Conference Key Agreement Protocols with Provable Security," in Proc. Asiacrypt 2000, 2000, vol. LNCS 1976, Lecture Notes in Computer Science, pp. 614-627.

[13] R. Dutta and R. Barua, "Provably Secure Constant Round Contributory Group Key Agreement in Dynamic Setting," IEEE Transactions on Information Theory, vol. 54, no. 5, 2007-2025, 2008.

[14] W.-G. Tzeng, "A Secure Fault-Tolerant Conference-Key Agreement Protocol," IEEE Transactions on Computers, vol. 51, no.4, pp. 373-379, 2002.

