ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Bi-Linear Approach for Efficient Encryption Using Short Ciphertexts

Bushra Fatima[1], Dr.Asma Parveen[2]

P G Student, Department of Computer Science and Engg, Khaja Banda Nawaz College of Engineering, Kalaburagi, India[1]

Head of the Department, Department of Computer Science and Engg, Khaja Banda Nawaz College of Engineering, Kalaburagi, India[2]

ABSTRACT: In a typical networking protocol a segregation of two or more keys under secure transmission is not achieved Broadcast Encryption (BE) schemes permit a sender to safely communicate to any subset of individuals yet requires a trusted party to circulate decryption keys. Group Key Agreement (GKA) protocol allows a group of members in an open network to agree to a common encryption key and only the members of the group are allowed to decrypt the ciphertexts, however a sender cannot eliminate any specific member from decrypting the ciphertexts. Here, we combine these two ideas with a hybrid primitive called as contributory broadcast encryption (ConBE). In this new primitive, a group of individuals settle to a common public encryption key while each individual holds a decryption key, hence the sender can confine the decryption to a subset of individuals of its choice. Following this, the ConBE scheme is proposed with short ciphertexts. In the standard model, this scheme is verified as collusion resistant under the n-Bilinear Diffie-Hellman Exponentiation (BDHE) assumption. From its independent significance, we show another BE scheme that is aggregatable. The aggregatability property appears to be helpful to build complex protocols.

KEYWORDS: Broadcast encryption;Group key agreement;Contributory broadcast encryption

I. Introduction

The phenomenal development of the web has expanded both the number and the prevalence of applications that require a reliable foundation for group communication. The quick progress and unavoidable arrangement of correspondence innovations, there is a great demand of adaptable cryptographic primitives to secure group communications at different platforms. New platforms involve ad hoc networks, social networks, cooperative computing and instant messaging tools. These new applications need the cryptographic primitives enabling a sender to safely encrypt to any subset of the clients of the administrations without depending on a third party. Broadcast encryption (BE) is a well understood primitive that is designed for secure group communications. It enables a sender to safely communicate with any subset of the group members.

Nevertheless, a BE framework vigorously depends on a completely trusted key server which produces secret decryption keys for the individuals and hence the communications of group members is not hidden. Group key agreement (GKA) is another well studied cryptographic primitive to secure group communications. A traditional GKA enables a group of members to set up a common secret key through open networks. In any case, if a sender wants to broadcast a message to a group, then the sender must join the group first and then run the GKA protocol for sharing secret key. Hence to overcome this limitation asymmetric GKA is introduced. But neither asymmetric GKA nor symmetric GKA are capable of excluding any particular member of the group from reading the message.

II. Literature survey

- Amos Fiat; Moni Naor, **"Broadcast encryption"** *Proc. Advances in Cryptology – CRYPTO '93* (Extended abstract). Lecture Notes in Computer Science. **773**: 480–491, 1994. Introduced new theoretical measures for the qualitative and quantitative assessment of encryption schemes designed for broadcast transmissions. The goal is to allow a central broadcast site to broadcast secure transmissions to an arbitrary set of recipients while minimizing key management related transmissions. We present several schemes that allow a center to broadcast a secret to any subset of privileged users out of a universe of size *n* so that coalitions of *k* users not in the privileged set cannot learn the secret.

- 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. Explained that encryption is used in a communication system to safeguard information in the transmitted messages from anyone other than the intended receiver(s). To perform the encryption and decryption the transmitter and receiver(s) ought to have matching encryption and decryption keys. A clever way to generate these keys is to use the public key distribution system invented by Diffie and Hellman. That system, however, admits only one pair of communication stations to share a particular pair of encryption and decryption keys, The public key distribution system is generalized to a conference key distribution system (CKDS) which admits any group of stations to share the same encryption and decryption keys.

- Q. Wu, Y. Mu, W. Susilo, B. Qin and J. Domingo-Ferrer, **"Asymmetric Group Key Agreement,"** in Proc. Eurocrypt 2009, vol. LNCS 5479, Lecture Notes in Computer Science, pp. 153-170, 2009. A group key agreement (GKA) protocol allows a set of users to establish a common secret via open networks. Observing that a major goal of GKAs for most applications is to establish a confidential channel among group members, we revisit the group key agreement definition and distinguish the conventional (symmetric) group key agreement from asymmetric group key agreement (ASGKA) protocols. Instead of a common secret key, only a shared encryption key is negotiated in an ASGKA protocol. This encryption key is accessible to attackers and corresponds to different decryption keys, each of which is only computable by one group member.

- Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and O. Farr`as, **"Bridging 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) schemes allow a sender to securely broadcast to any subset of members but requires a trusted party to distribute decryption keys. Group key agreement (GKA) protocols enable a group of members to negotiate a common encryption key via open networks so that only the members can decrypt the ciphertexts encrypted under the shared encryption key, but a sender cannot exclude any particular member from decrypting the ciphertexts. In this paper, we bridge these two notions with a hybrid primitive referred to as contributory broadcast encryption (CBE). In this new primitive, a group of members negotiate a common public encryption key while each member holds a decryption key. A sender seeing the public group encryption key can limit the decryption to a subset of members of his choice. Following this model, we propose a CBE scheme with short ciphertexts. The scheme is proven to be fully collusion-resistant under the decision n-Bilinear Diffie-Hellman Exponentiation (BDHE) assumption 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 includes three entities: the group manager dealing with membership, the encryptor encrypting the data for registered clients according to a specific policy (the target set), and the users that decrypt the message if they are authorized. Public-key broadcast encryption is capable of excluding this unique role of encryptor, by permitting a body to send encrypted data. We go a step further in the decentralization process, by removing the group manager, as well as the addition of further members to the system, do not require any central authority. Our construction makes black-box use of well-known primitives and can be considered as an extension to the subset-cover framework.

III. EXISTING METHODOLOGY

In the existing system, Group key agreement (GKA) is a well studied cryptographic primitive for secured group communications. A regular GKA enables a group of individuals to set up a typical secret key through open networks. Nevertheless, if a sender wants to send a message in the group then it should first join the group and run the GKA protocol to distribute the secret key to the particular members. However, to overcome this drawback, Wu et al.

presented asymmetric GKA, in which just a typical group key is negotiated and each individual holds a different key for decryption. However, neither symmetric GKA nor the recently presented asymmetric GKA enable the sender to eliminate a specific member from reading the plaintext. Henceforth, it is important to discover more adaptable cryptographic primitives permitting dynamic communication without a completely trusted third party.

IV. PROPOSED WORK

In the proposed work, we show the Contributory Broadcast Encryption (ConBE) primitive, which is a half and half of GKA and BE. It gives security proofs, represents the need of the aggregatability of the hidden BE building block and demonstrates the reasonableness of ConBE scheme with investigations. First, we display the ConBE primitive and formalize its security definitions. ConBE deals with the idea of both GKA and BE. A group of individuals connect through open networks to settle a public encryption key while each individual holds a different key for decryption. Utilizing this public encryption key, anybody can encrypt any message to any subset of the group individuals and just the selected recipients can decrypt. We formalize resistance of collusion by characterizing an attacker who can completely control all the individuals outside the desired recievers yet can't extricate information from the ciphertext. Second, we introduce the idea of aggregatable broadcast encryption (AggBE). Roughly, a BE scheme is said to be aggregatable if its safe cases can be aggregated into another protected case of the BE scheme. In particular, just the aggregated decryption keys of a similar client are valid decryption keys relating to the aggregatable public keys of the fundamental BE instances. Finally, we develop a productive ConBE scheme with our AggBE as a building block. The ConBE development in the standard model is said to be semi-adaptively secure under the BDHE assumption

System Architecture

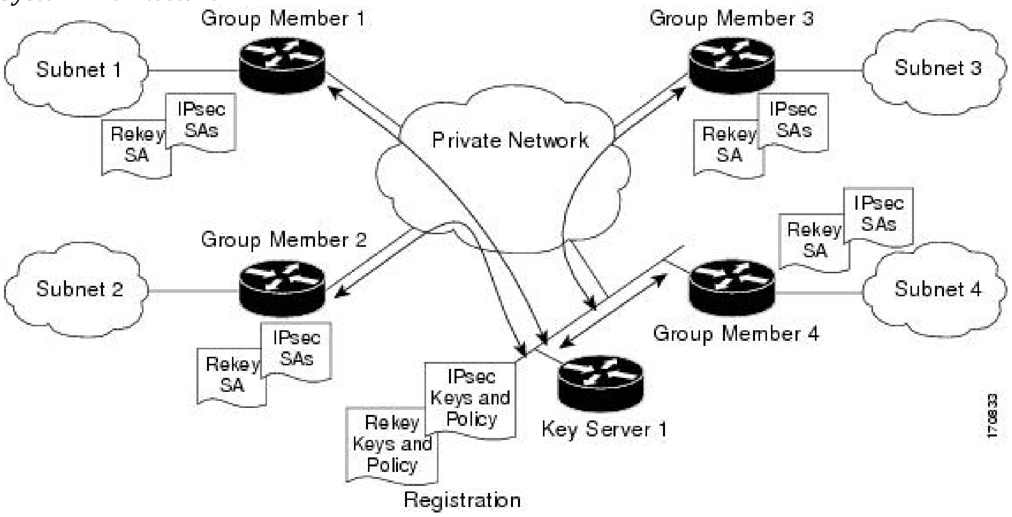

Figure 1: System architecture of the ConBE

In figure 1 system architecture at high level includes two fundamental strategies for this group encryption service are Encrypt (set, m) c: where set is an group of members to which the message m is to be encrypted. This technique restores the relating ciphertext c Decrypt (c) (m or error status): where c is the ciphertext and m is the subsequent decryption. In the event if decryption fails, an error code is returned. Depending upon the implementation, ciphertext c may have certain structure, for example, contains the identity or details of the sender, the key encapsulation block, the encryption of the message under the encapsulated key, the block of signature, and so forth. Additionally, different strategies can be presented to the application, they are, AddUserCertificate and RemoveUserCertificate. It might likewise be helpful to enable the application to utilize named groups rather than sets in Encrypt (group, m); if this technique is used it should be accompanied with the group management strategies, they are: NewGroup, AddMember, and RemoveMember.

V. RESULTS

Results involve both data efficiency and time efficiency graph. Figure 2 illustrates the data efficiency of the proposed system increased compared to the existing system and figure 3 shows the encryption/decryption time for online session key. Here, we see that time is around steady for various group sizes, which is constant with theoretical analysis. Both session key encryption and session key decryption take the time below 10ms for 80-bit security level, and takes below 80ms for 128-bit security level. After the set up of the system, the session key transmission is efficient, which is convenient and absolutely makes the ConBE scheme practical.

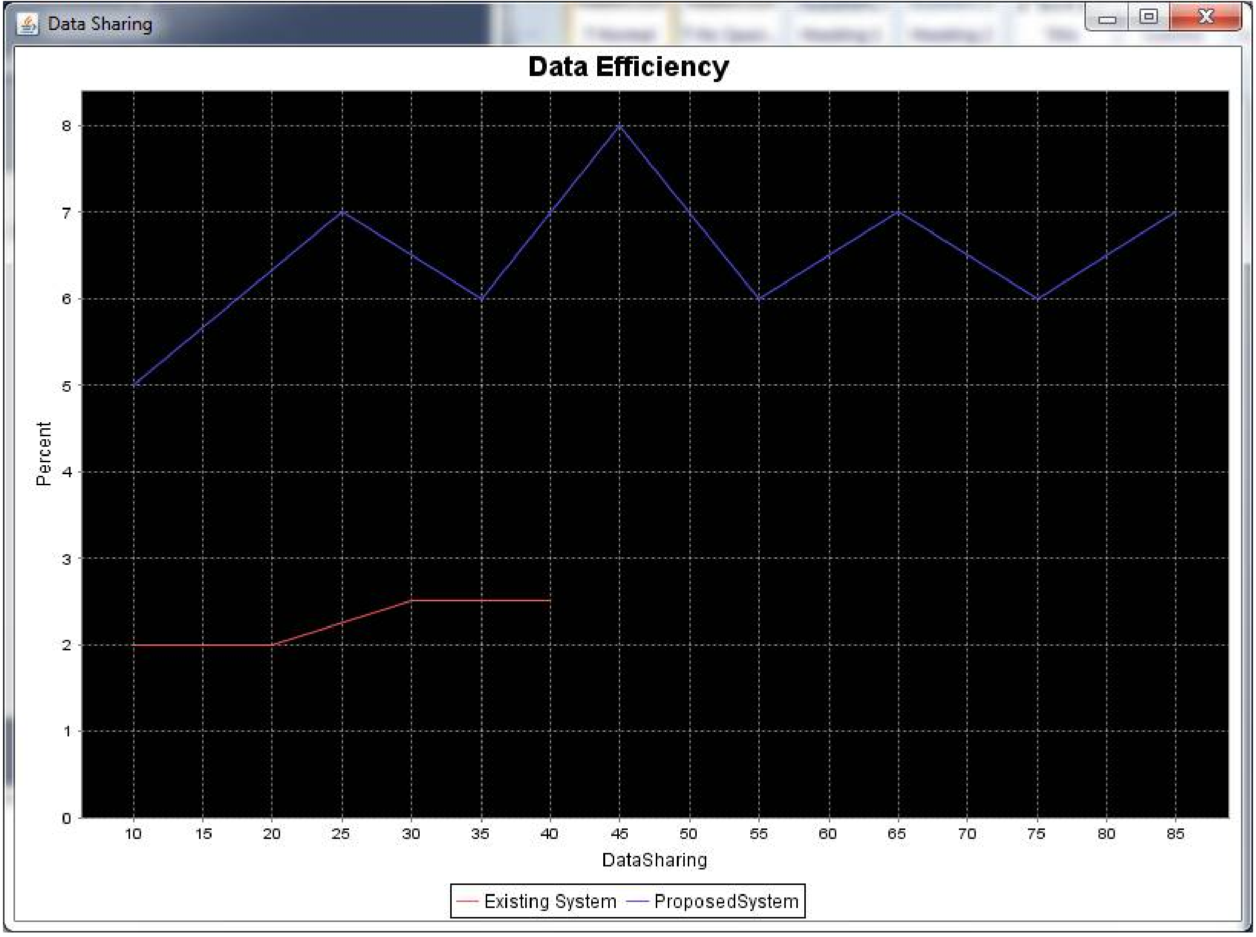

Figure 2: Data Efficiency graph

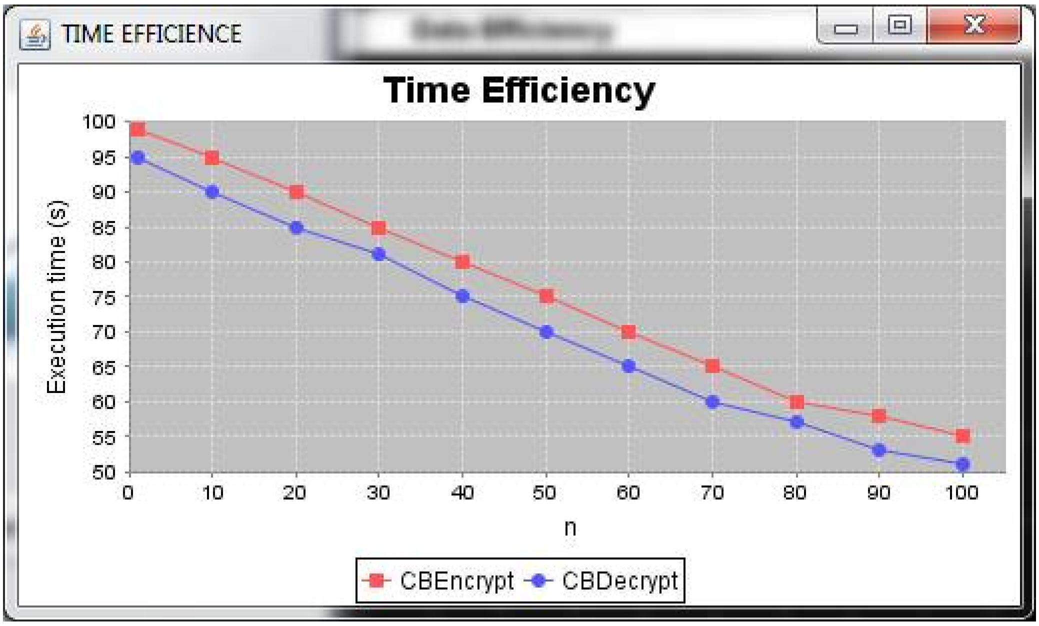

Figure 3: Time Efficiency graph

VI. CONCLUSION AND FUTURE WORK

In this proposed work, we analysed the ConBE scheme. In ConBE, any individual can send secret messages to any subset of the group members, and there is no need of involving a trusted key server. Neither any change in the sender nor the dynamic choice of the intended receivers needs additional rounds to settle group encryption/decryption keys. Following the ConBE model, we instantiated a proficient ConBE scheme that is safe in the standard model. As a flexible cryptographic primitive, our novel ConBE concept opens a new way to set up secure broadcast channels and communications and can be likely to secure various developing distributed computation applications.

REFERENCES

[1] A. Fiat and M. Naor, "Broadcast Encryption," in Proc. Crypto 1993, Lecture Notes in Computer Science, vol. LNCS 773, pp. 480-491, 1994.
[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, Lecture Notes in Computer Science, vol. LNCS 5479, pp. 153-170,2009.
[4] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and O. Farr`as, "Bridging Broadcast Encryption and Group Key Agreement," in Proc. Asiacrypt 2011, Lecture Notes in Computer Science, vol. LNCS 7073, pp. 143-160, 2011.
[5] D. H. Phan, D. Pointcheval and M. Strefler, "Decentralized Dynamic Broadcast Encryption," in Proc. SCN 2012, , Lecture Notes in Computer Science, vol. LNCS 7485, pp. 166-183, 2011.
[6] 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.
[7] 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.
[8] 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.*
[9] 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.*
[10] C. Boyd and J.M. Gonz´alez-Nieto, *"Round-Optimal Contributory Conference Key Agreement," in Proc. PKC 2003, , Lecture Notes in Computer Science, vol. LNCS 2567, pp. 161-174, 2003..*
[11] W.-G. Tzeng and Z.-J. Tzeng, *"Round Efficient Conference Key Agreement Protocols with Provable Security," in Proc. Asiacrypt 2000, , Lecture Notes in Computer Science, vol. LNCS 1976, pp. 614-627, 2000.*
[12] 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, pp. 2007-2025, 2008.*
[13] W.-G. Tzeng *"A Secure Fault-Tolerant Conference-Key Agreement Protocol," IEEE Transactions on Computers, vol. 51, no.4, pp. 373-379, 2002.*