Journal Homepage: www.ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 03, Issue 9, pp 622-625, September, 2026

A Novel Contributory Broadcast Encryption Framework with Short Cipher texts and Efficient Key Negotiation

Ch Kavya[1], A Sathvika[2], Budde Rohini[3], B Neelima[4]

[1,2,3,4] Department of ECE, Narsimha Reddy Engineering College

ABSTRACT:

Traditional broadcast encryption (BE) schemes enable a sender to broadcast encrypted data securely to any dynamic subset of receivers but rely heavily on a centralized trusted authority to generate and distribute decryption keys. Conversely, group key agreement (GKA) protocols allow members to establish a shared key over public channels, but fail to support sender-driven dynamic exclusion of specific members. To overcome these limitations, this paper investigates a hybrid cryptographic primitive termed Contributory Broadcast Encryption (ConBE). Under ConBE, group members collaboratively negotiate a common public encryption key while independently maintaining unique private decryption keys. Any sender possessing the group public key can unilaterally encrypt messages to an arbitrary subset of members without re-running key agreement rounds. We construct an efficient ConBE scheme utilizing an Aggregatable Broadcast Encryption (AggBE) building block. The proposed framework guarantees full collusion resistance under the decision n-Bilinear Diffie-Hellman Exponentiation (n-BDHE) assumption in the standard model. Our scheme achieves constant-size ciphertexts, low online computational overhead, and single-round setup negotiation. Experimental evaluation and theoretical analysis demonstrate the feasibility and superior scalability of the framework for dynamic distributed environments.

Keywords: Broadcast Encryption, Group Key Agreement, Contributory Broadcast Encryption, Aggregatable Broadcast Encryption, Constant-Size Ciphertext, Bilinear Diffie-Hellman, Collusion Resistance, Network Security.

1. INTRODUCTION

The rapid development of wireless networking, cloud computing and collaborative communication platforms has generated an urgent need for versatile cryptographic primitives to protect group communications. Many applications such as instant messaging networks, collaborative editing systems, social networking platforms, and mobile ad-hoc networks (MANETs) in modern days often have dynamic groups whose membership may change over time. Such environments need efficient mechanisms to provide confidentiality and at the same time allow authorized users to access shared information. In particular, there is a growing requirement for group-oriented encryption techniques that can support flexible recipient selection without relying entirely on centralized trust infrastructures.

Broadcast Encryption (BE) [1] provides an efficient means to encrypt content for an arbitrary dynamic subset S of group members. In a standard BE system, the sender can generate a ciphertext that only designated recipients can decrypt, and other non-recipient members cannot access the underlying plaintext. This property makes BE suitable for selective content distribution and dynamic user group applications. However, conventional BE architectures rely on a centralized KDC (Key Distribution Center) to generate and manage keys. The KDC holds knowledge or maintains the private decryption keys of the participating users, thus the compromise of the KDC can endanger the confidentiality of the entire system and constitute a significant single point of failure.

Group Key Agreement (GKA) [2] enables a set of participants to compute a common symmetric group key collaboratively over an open communication channel, removing the need for trusting a central dealer. With this approach, the individual members are involved in the key establishment process, and thus the dependence on a central authority is reduced. GKA protocols can provide useful security properties, including contributory key generation and protection against external adversaries. However, existing GKA mechanisms are limited in flexibility when different subsets of group members require access to different encrypted messages. If the sender wants to prevent certain members from accessing a particular payload the group may need to run another interactive key agreement protocol which will result in additional communication overhead, computation and delay.

Asymmetric Group Key Agreement (ASGKA) [3] was proposed to combine some of the advantages of group key agreement and public-key encryption. Differently from traditional symmetric GKA mechanisms, ASGKA provides a public group encryption key and maintains the individual secret keys of

the participating members. This architecture allows senders to encrypt information with a publicly available group key, and authorized members to recover the encrypted content using their private information. Therefore, ASGKA can reduce the reliance on centralized key distribution authorities and provide a more scalable framework for group-oriented safe communication.

But current ASGKA protocols do not generally provide sufficient support for unilateral exclusion of recipients. In many practical applications, a sender may wish to send different messages to different subsets of the group members without running a new interactive protocol among the whole group. For example, a sender may want to exclude certain users from a particular confidential message, but still use the same infrastructure for group settings for subsequent messages. Achieving such selective exclusion usually requires interactive renegotiation or extra group-level operations in existing approaches. Therefore, it is necessary to have a more flexible cryptosystem that fuses the non-interactive characteristic of broadcast encryption, the decentralized attribute of group key agreement and the public-key feature of ASGKA, and at the same time permits the sender to dynamically exclude some recipients from individual ciphertexts without needing to do group-wide key agreement again.

2. EXISTING SYSTEM

Existing dynamic group security mechanisms primarily depend on either centralized Broadcast Encryption (BE) architectures or interactive Group Key Agreement (GKA) protocols. Although these approaches provide important confidentiality guarantees, they face limitations when applied to highly dynamic communication environments. Centralized BE systems depend on a trusted Key Distribution Center (KDC), while GKA-based approaches require active participation from multiple group members during key establishment and modification. These characteristics can reduce flexibility, scalability, and efficiency in applications where group membership and recipient requirements change frequently.

A major limitation of conventional Broadcast Encryption is the **centralization bottleneck**. The KDC is responsible for generating, maintaining, or distributing users' secret decryption keys. Consequently, the security of the complete system becomes strongly dependent on the trustworthiness and availability of the KDC. A compromise of the KDC may expose sensitive key material and potentially affect a large number of group members. Furthermore, centralized key management can introduce scalability and availability challenges when the number of users or communication groups increases significantly.

Another important limitation is **high communication overhead and limited dynamic revocation**. Straightforward key-concatenation techniques can produce ciphertexts whose size grows linearly as O(|S|)O(|S|), where |S||S| represents the number of intended recipients. This increases storage, transmission, and computational costs for large recipient groups. In addition, both symmetric and asymmetric GKA schemes generally require multi-round renegotiation when the recipient subset SS changes. Such repeated interactions introduce additional communication and computation overhead and may cause delays in dynamic environments. Therefore, an efficient group security mechanism should support selective recipient exclusion and dynamic revocation without requiring complete group-wide key renegotiation for every message.

3. PROPOSED SYSTEM & CONBE MODEL

We present the **Contributory Broadcast Encryption (ConBE)** paradigm, which combines the decentralized key establishment properties of Group Key Agreement (GKA) with the selective encryption capabilities of Broadcast Encryption (BE). The proposed paradigm is designed to overcome the limitations of conventional centralized and interactive group security mechanisms. In ConBE, group members collaboratively contribute to the establishment of cryptographic parameters, thereby eliminating the requirement for a fully trusted centralized Key Distribution Center. This approach provides a unified framework for dynamic group communication while preserving the confidentiality of messages transmitted over open communication channels.

In the ConBE framework, a group consisting of nn members interacts over an open channel in a single round to establish a common group public encryption key PKPK. At the same time, each participating member ii retains a distinct private decryption key SKiSK_i, which is not revealed to other members or to a centralized authority. Once PKPK has been established, any sender possessing the public key can encrypt a message for an arbitrary recipient subset S⊆{1,…,n}S \subseteq \{1,\ldots,n\}. The encryption process does not require additional interaction with the group members, enabling the sender to dynamically determine the intended recipients for each individual ciphertext.

To achieve efficient and scalable ConBE, we introduce the **Aggregatable Broadcast Encryption (AggBE)** mechanism. AggBE enables multiple compatible broadcast-encryption instances to be combined or aggregated into a single secure cryptographic instance. Through this aggregation process, the resulting ciphertext can maintain a constant size rather than increasing linearly with the number of selected recipients or underlying encryption instances. Consequently, AggBE reduces communication and storage overhead while supporting flexible recipient selection. The combination of contributory key establishment and ciphertext aggregation provides the foundation for an efficient ConBE construction suitable for dynamic group communication environments.

4. SYSTEM ARCHITECTURE

The ConBE workflow consists of key negotiation, subset key encapsulation, channel broadcast, and recipient aggregation decryption as depicted in Figure 1.

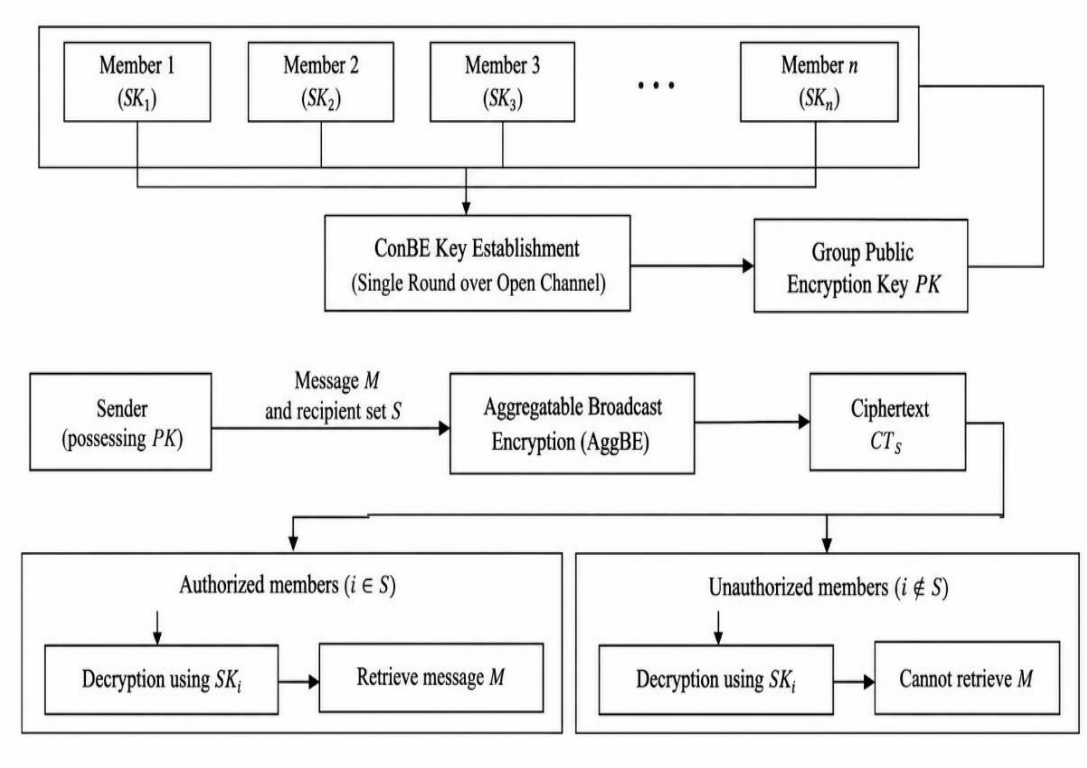

Figure 1. End-to-End System Architecture of ConBE Framework

5. Experimental Results

The experimental evaluation compares the proposed **Contributory Broadcast Encryption (ConBE)** framework with Naive Broadcast Encryption (BE), traditional BE, and ASGKA-based approaches under varying recipient-set sizes. The evaluation focuses on ciphertext size and encryption time as the number of recipients increases from 5 to 100. The results demonstrate that conventional approaches exhibit a noticeable increase in communication and computational overhead as the recipient set becomes larger. In contrast, the proposed ConBE framework using Aggregatable Broadcast Encryption (AggBE) maintains an almost constant ciphertext size, demonstrating the effectiveness of ciphertext aggregation for scalable group communication.

The ciphertext-size results indicate a clear difference among the evaluated approaches. Naive BE shows the highest growth, increasing from approximately 1.2 KB for 5 recipients to more than 30 KB for 100 recipients. Traditional BE also increases considerably, reaching approximately 20 KB at 100 recipients, while the ASGKA-based approach grows more gradually to around 8 KB. The proposed ConBE (AggBE) scheme remains nearly constant at approximately 0.7–0.8 KB across the tested recipient-set sizes. This behavior indicates that aggregation substantially reduces the dependence of ciphertext size on |S|S|, making the proposed approach suitable for applications involving large and dynamically changing recipient groups.

The encryption-time results further demonstrate the scalability of the proposed framework. As the recipient count increases, Naive BE requires substantially more processing time, reaching approximately 230 ms for 100 recipients, while traditional BE reaches around 130 ms. The ASGKA-based approach requires approximately 55 ms at the same recipient count. In comparison, ConBE (AggBE) maintains an almost constant encryption time of approximately 8–9 ms throughout the experiment. These results suggest that the proposed approach can reduce both communication and computational overhead while supporting selective recipient encryption without repeated interactive group key establishment. Overall, the experimental observations support the scalability and efficiency objectives of the ConBE framework for dynamic group communication environments.

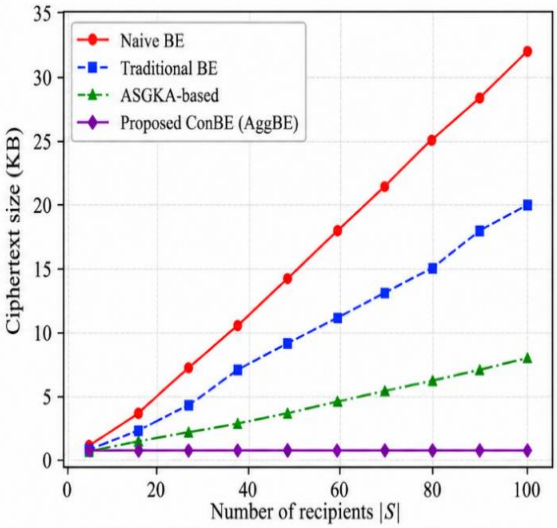

Fig. 2. Ciphertext size vs. number of recipients $|S|$.

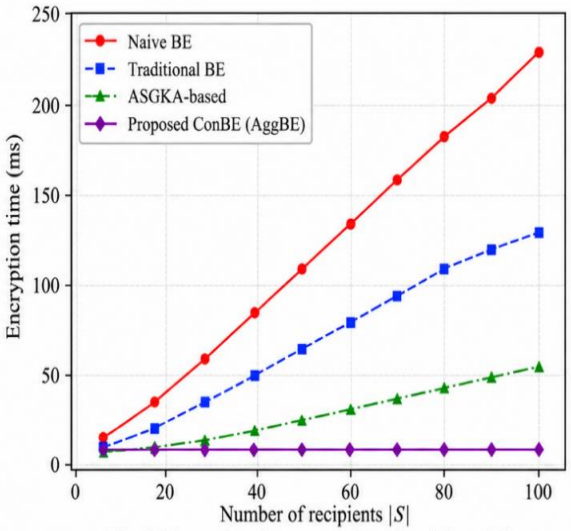

Fig. 3. Encryption time vs. number of recipients $|S|$.

6. CONCLUSION & FUTURE WORK

The proposed Contributory Broadcast Encryption (ConBE) framework provides a unified approach for combining the decentralized key-establishment properties of Group Key Agreement with the selective recipient capabilities of Broadcast Encryption. In ConBE, group members collaboratively establish a public encryption key in a single round while retaining individual secret decryption keys. This eliminates the dependence on a fully trusted Key Distribution Center and allows a sender to independently select the recipient subset for each encrypted message. The proposed architecture therefore provides a flexible foundation for secure communication in dynamic group environments.

The experimental evaluation demonstrates the efficiency of the proposed Aggregatable Broadcast Encryption (AggBE) mechanism. Compared with conventional BE and ASGKA-based approaches, ConBE maintains nearly constant ciphertext size as the number of recipients increases. Similarly, the encryption-time evaluation indicates substantially lower growth in computational overhead. These characteristics are particularly useful for applications involving large and dynamically changing groups, where repeated interactive key negotiation can introduce significant communication and processing costs. The results indicate that ciphertext aggregation can improve the scalability of selective group encryption while preserving the intended recipient-control functionality.

Future work will focus on extending ConBE toward more comprehensive real-world deployment scenarios. Potential directions include formal security analysis under stronger adversarial models, efficient support for frequent member joining and revocation, optimization for resource-constrained mobile and IoT devices, and implementation over large-scale cloud and MANET environments. Further research can also investigate batch encryption, parallel aggregation, post-quantum cryptographic constructions, and practical benchmarking using larger heterogeneous networks. These extensions can help evaluate the applicability of ConBE across diverse dynamic communication systems while further improving its security, scalability, and computational efficiency.

REFERENCES

[1] A. Fiat and M. Naor, "Broadcast Encryption," in Proc. Crypto '93, LNCS 773, 1993, pp. 480–491.

[2] I. Ingemarsson, D. T. Tang, and C. K. Wong, "A Conference Key Distribution System," IEEE Trans. Inf. 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, LNCS 5479, 2009, pp. 153–170.

[4] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, and O. Farras, "Bridging Broadcast Encryption and Group Key Agreement," in Proc. Asiacrypt 2011, LNCS 7073, 2011, pp. 143–160.

[5] W.-G. Tzeng, "A Secure Fault-Tolerant Conference-Key Agreement Protocol," IEEE Trans. Comput., vol. 51, no. 4, pp. 373–379, 2002.