ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 12, March 2016

DECENTRALIZED BROADCAST ENCRYPTION USING GROUP KEY AGREEMENT

Kanagavalli.M [1], Matheswaran.V [2]

1. P.G. Student, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India
2. Asst.Professor, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India

Abstract: Traditional broadcast encryption (BE) schemes allow a sender to securely broadcast to any subset of members but require 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 group 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 (ConBE). 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 ConBE 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. Of independent interest, we present a new BE scheme that is aggregatable. The aggregatability property is shown to be useful to construct advanced protocols.

Index Terms—Broadcast encryption, group key agreement, contributory broadcast encryption, provable security.

I. INTRODUCTION

With the fast advance and pervasive deployment of communication technologies, there is an increasing demand of versatile cryptographic primitives to protect group communications and computation platforms. These new platforms include instant-messaging tools, collaborative computing, mobile ad hoc networks and social networks. These new applications call for cryptographic primitives allowing a sender to securely encrypt to any subset of the users of the services without relying on a fully trusted dealer. Broadcast encryption (BE) [1] is a well-studied primitive intended for secure group-oriented communications. It allows a sender to securely broadcast to any subset of the group members. Nevertheless, a BE system heavily relies on a fully trusted key server who generates secret decryption keys for the members and can read all the communications to any members. Group key agreement (GKA) is another well-understood cryptographic primitive to secure group-oriented communications. A conventional GKA [2] allows a group of members to establish a common secret key via open networks. However, whenever a sender wants to send a message to a group, he must first join the group and run a GKA protocol to share a secret key with the intended members. More recently, and to overcome this limitation, Wu et al. introduced asymmetric GKA [3], in which only a common group public key is negotiated and each group member holds a different decryption key. However, neither conventional symmetric GKA nor the newly introduced asymmetric GKA allow the sender to unilaterally exclude any particular member from reading the plaintext.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 12, March 2016

Hence, it is essential to find more flexible cryptographic primitives allowing dynamic broadcasts without a fully trusted dealer. We present the Contributory Broadcast Encryption (ConBE) primitive, which is a hybrid of GKA and BE. 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. Unlike GKA, ConBE allows the sender to exclude some members from reading the ciphertexts. Christo Ananth et al. [7] proposed a system which contributes the complex parallelism mechanism to protect the information by using Advanced Encryption Standard (AES) Technique. AES is an encryption algorithm which uses 128 bit as a data and generates a secured data. In Encryption, when cipher key is inserted, the plain text is converted into cipher text by using complex parallelism. Similarly, in decryption, the cipher text is converted into original one by removing a cipher key. The complex parallelism technique involves the process of Substitution Byte, Shift Row, Mix Column and Add Round Key. The above four techniques are used to involve the process of shuffling the message. The complex parallelism is highly secured and the information is not broken by any other intruder. The proposed AggBE scheme offers efficient encryption/decryption and short ciphertexts. 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. Only one round is required to establish the public group encryption key and set up the ConBE system. After the system set-up, the storage cost of both the sender and the group members is O(n), where n is the number of group members participating in the setup stage. However, the online complexity (which dominates the practicality of a ConBE scheme) is very low. We also illustrate a trade-off between the set-up complexity and the online performance. After a trade-off, the variant has O (n2=3) complexity in communication, computation and storage. This is comparable to up-to-date regular BE schemes which have O(n1=2) complexity in the same performance metrics, but our scheme does not require a trusted key dealer. We conduct a series of experiments and the experimental results validate the practicality of our scheme.

II RELATED WORK

A number of works have addressed key agreement protocols for multiple parties. The schemes due to Ingemarsson et al. [2] and Steiner et al. are designed for n parties and require O(n) rounds. Tree key structures have been further proposed, reducing the number of rounds to O(log n) [8], [9], [10]. Multi-round GKA protocols pose a synchronism requirement: in order to complete the protocol, all the group members have to stay online simultaneously. How to optimize the round complexity of GKA protocols has been studied in several works (e.g., [11], [12], [13]). In [14], Tzeng presented a constant-round GKA protocol that can identify cheaters. Subsequently, Yi [15] constructed a fault-tolerant protocol in an identity-based setting. Burmester and Desmedt [16] proposed a two-round n-party GKA protocol for n parties. The Joux protocol [17] is one-round and

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 12, March 2016

only applicable to three parties. The work of Boneh and Silverberg [18] shows a one-round (n+1)-party GKA protocol with n-linear pairings. Dynamic GKA protocols provide extra mechanisms to handle member changes. Bresson et al. [19], [20] extended the protocol in [21] to dynamic GKA protocols that allow members to leave and join the group. The number of rounds in the set-up/join algorithms of the Bresson et al.'s protocols [19], [20] is linear with the group size, but the number of rounds in the leave algorithm is constant. The theoretical analysis in [22] shows that for any tree-based group key agreement scheme, the lower bound of the worst-case cost is O(log n) rounds of interaction for a member to join or leave. Without relying on a tree-based structure, Kim et al. [23] proposed a two-round dynamic GKA protocol. Recently, Abdalla et al. [24] presented a two-round dynamic GKA protocol in which only one round is required to cope with the change of members if they are in the initial group. Jarecki et al. [25] presented a robust two-round GKA protocol in which a session key can be established even if some participants fail during the execution of the protocol. Observing that existing GKA protocols cannot handle sender/member changes efficiently, Wu et al. Presented a group key management protocol [26] in which a change of the sender or monotone exclusion of group members does not

require extra communication, and changes of other members require one extra round. BE is another well-established cryptographic primitive developed for secure group communications. As the core of BE is to generate and distribute the key materials to the participants, BE schemes are also referred to as key distribution schemes in some scenarios. While digital rights management motivated most previous BE schemes recent efforts are devoted to modifying BE or key distribution technologies in view of securing emerging information systems such as sensor networks, mobile ad hoc networks, vehicular networks, etc. BE schemes in the literature can be classified into two categories, i.e., symmetric-key BE [1] and public-key BE. In the symmetric-key setting, only the trusted center generates all the secret keys and broadcasts messages to users. Hence, only the key generation center can be the broadcaster or the sender. Similarly to the GKA setting, tree-based key structures were independently proposed to improve efficiencyin symmetric-key BE systems, and further improved in with O(log n) keys. Cheon et al. presented an efficient symmetric BE scheme allowing new members to join the protocol anytime. Harn and Lin proposed a group key transfer protocol. Their protocol is based on secret sharing and is considerably efficient, albeit it cannot revoke (compromised) users. In the public-key BE setting, the trusted center also generates a public key for all the users so that any one can play the role of a broadcaster or sender. Naor and Pinkas presented in the first public-key BE scheme in which up to a threshold of users can be revoked. Subsequently, presented a fully collusion-resistant public-key BE scheme exploiting new bilinear pairing technologies in which the key size, the ciphertext size, and the computation costs are O(pn).

The scheme in slightly reduces the size of the key and the ciphertexts, although it still has sub-linear complexity. The schemes presented in strengthen the security concept of public-key BE schemes. As to performance, the sub-linear barrier O(pn) has not yet been broken. In Lewko et al. proposed two elegant schemes with constant public and secret

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 12, March 2016

keys, although their ciphertext size is linear with the number of the revoked users, which is O(n) in the worst case.

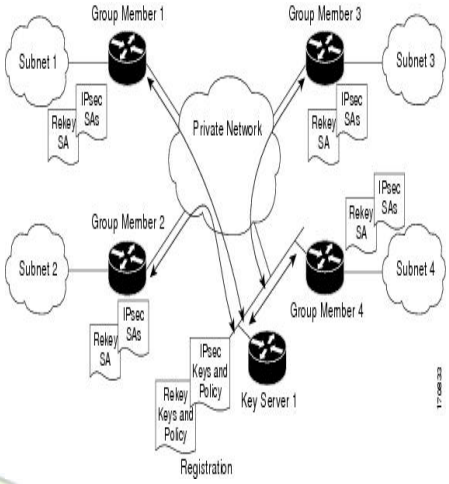
2.1 Existing System:

- Group key agreement (GKA) is another well-understood cryptographic primitive to secure group-oriented communications. A conventional GKA allows a group of members to establish a common secret key via open networks. However, whenever a sender wants to send a message to a group, he must first join the group and run a GKA protocol to share a secret key with the intended members.
- More recently, and to overcome this limitation, Wu et al. introduced asymmetric GKA, in which only a common group public key is negotiated and each group member holds a different decryption key.
- However, neither conventional symmetric GKA nor the newly introduced asymmetric GKA allow the sender to unilaterally exclude any particular member from reading the plaintext. Hence, it is essential to find more flexible cryptographic primitives allowing dynamic broadcasts without a fully trusted dealer.

2.1.1 Disadvantages of Existing System:

- Need a fully trusted third party to set up the system.
- Existing GKA protocols cannot handle sender/member changes efficiently.

III. SYSTEM ARCHITECTURE



At the high-level, two main methods of this group encryption service are

Encrypt(set, m) c : where set is a set of participant identifiers to which message m is to be encrypted. This method returns the corresponding ciphertext c

Decrypt (c) (m or error status): where c is the ciphertext and m is the resulting decryption. If decryption fails, an appropriate error code is returned. Depending on the implementation, ciphertext c may have certain structure, such as include the identity of the sender, the key encapsulation block, the encryption of the message under the encapsulated key, the signature block, etc.

In addition to these two main methods, other methods can be exposed to the application, such as *AddUserCertificate and RemoveUserCertificate.* It may also be convenient to allow the application to use named groups instead of sets in Encrypt(group, m) ; if this method is provided it needs to be accompanied with the following group management methods: *NewGroup , AddMember, , and RemoveMember*

Security Properties:

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 12, March 2016

Confidentiality: Communicated data is protected from non-members.

Sender authentication and non-repudiation: Participants can authenticate message senders.

Membership dynamism: It is possible to form groups and to add/remove participants.

Perfect Forward Security: Compromise of long term keys of a member does not compromise earlier communication of that member.

Group Forward and Backward Secrecy:Secrecy of new communication from revoked members, and old communication from new members.

3.1 Modules Description

- Network Environment Setup Module
- Certificate Authority Module
- Key Broadcast Module
- Group Key management

3.1.1 Network Environment Setup Module: In the first module, we create the network environment setup with nodes, certificate authority. Network environment is set up with nodes connected with all and using socket programming in java.

3.1.2 Certificate Authority Module: In this module, each receiver has a public/secret key pair. The public key is certified by a certificate authority, but the secret key is kept only by the receiver. A remote sender can retrieve the receiver's public key from the certificate authority and validate the authenticity of the public key by checking its certificate, which implies that no direct communication from the receivers to the sender is necessary. Then, the sender can send secret messages to any chosen subset of the receivers.

3.1.3. Key Broadcast Module: In this module formally define the model of group key agreement-based broadcast encryption. The definition incorporates the up-to-date definitions of group key agreement and public-key broadcast encryption. Since the core of key management is to securely distribute a session key to the intended receivers, it is sufficient to define the system as a session key encapsulation mechanism. Then, the sender can simultaneously encrypt any message under the session key, and only the intended receivers can decrypt. The new paradigm seems to require a trusted third party as its counterpart in traditional broadcast encryption systems. A closer look shows there is a difference. In a traditional broadcast encryption system, the third party has to be fully trusted, that is, the third party knows the secret keys of all group members and can read any transmission to any subgroup of the members. This kind of fully trusted third party is hard to implement in open networks. In contrast, the third party in our key management model is only partially trusted. In other words, the third party only knows and certifies the public key of each member. This kind of partially trusted third party has been implemented and is known as public key infrastructure (PKI) in open networks.

3.1.4 Group Key management : The new key management paradigm ostensibly requires a sender to know the keys of the receivers, which may need communications from the receivers to the sender as in traditional group key agreement protocols. However, some subtleties must be pointed out here. In traditional group key agreement protocols, the sender has to simultaneously stay online with the receivers and direct communications from the receivers to the sender are needed. This is difficult for a remote sender. On the contrary, in our key

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 12, March 2016

management paradigm, the sender only needs to obtain the receivers' public keys from a third party, and no direct communication from the receivers to the sender is required, which is implementable with exactly the existing PKIs in open networks. Hence, this is feasible for a remote sender. In our scheme, it is almost free of cost for a sender to exclude a group member by deleting the public key of the member from the public key chain or, similarly, to enroll a user as a new member by inserting that user's public key into the proper position of the public key chain of the receivers. After the deletion/addition of certain member, a new logical public-key ring naturally forms. Hence, a trivial way to enable this change is to run the protocol independently with the new key ring. If the sender would like to include a new member, the sender just needs to retrieve the public key of this user and insert it into the public key chain of the current receiver set. By repeatedly invoking the member addition operation, a sender can merge two receiver sets into a single group. Similarly, by repeatedly invoking the member deletion operation, a sender can partition one receiver set into two groups. Both merging and partitioning can be done efficiently. In this module shows the deletion of member from the receiver group. Then, the sender and the remaining receivers need to apply this change to their subsequent encryption and decryption procedures.

3.2 PROPOSED SYSTEM

- 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.

3.2.1 Advantages of Proposed System

- We construct a concrete AggBE scheme tightly proven to be fully collusion-resistant under the decision BDHE assumption.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 12, March 2016

- The proposed AggBE scheme offers efficient encryption/decryption and short ciphertexts.
- Only one round is required to establish the public group encryption key and set up the ConBE system.

IV. CONCLUSIONS

In this paper, we formalized the ConBE primitive. In ConBE, anyone can send secret messages to any subset of the group members, and the system does not require a trusted key server. Neither the change of the sender nor the dynamic choice of the intended receivers requires extra rounds to negotiate group encryption/decryption keys. Following the ConBE model, we instantiated an efficient ConBE scheme that is secure in the standard model. As a versatile cryptographic primitive, our novel ConBE 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] Christo Ananth, H.Anusuya Baby, "High Efficient Complex Parallelism for Cryptography", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. III (Mar-Apr. 2014), PP 01-07

[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.

[15] X. Yi, "Identity-Based Fault-Tolerant Conference Key Agreement," IEEE Transactions Dependable Secure Computing vol. 1, no. 3, 170-178, 2004.

[16] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System," in Proc. Eurocrypt 1994, 1994, vol. LNCS 950, Lecture Notes in Computer Science, pp. 275-286.

[17] A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman," Journal of Cryptology, vol. 17, no. 4, pp. 263-276, 2004.

[18] D. Boneh and A. Silverberg, "Applications of Multilinear Forms to Crytography," Contemporary Mathematics, vol. 324, pp.71-90, 2003.

[19] E. Bresson, O. Chevassut and D. Pointcheval, "Provably Authenticated Group Diffie-Hellman Key Exchange – The Dynamic Case," in Proc. Asiacrypt 2001, 2001, vol. LNCS 2248, Lecture Notes in Computer Science, pp. 290-309.

[20] E. Bresson, O. Chevassut and D. Pointcheval, "Dynamic Group Diffie- Hellman Key Exchange under Standard Assumptions," in Proc. Eurocrypt 2002, 2002, vol. LNCS 2332, Lecture Notes in Computer Science, pp. 321-336.

[21] E. Bresson, O. Chevassut, D. Pointcheval and J.-J. Quisquater, "Provably Authenticated Group Diffie-Hellman Key Exchange," in Proc. ACM CCS 2001, 2001, pp. 255-264.

[22] J. Snoeyink, S. Suri and G. Varghese, "A Lower Bound for Multicast Key Distribution," in Proc. INFOCOM 2001, 2001, pp. 422-431.

[23] H.J. Kim, S.M. Lee and D. H. Lee, "Constant-Round Authenticated Group Key Exchange for Dynamic Groups," in Proc. Asiacrypt 2004,2004, vol. LNCS 3329, Lecture Notes in Computer Science, pp. 245-259.

[24] M. Abdalla, C. Chevalier, M. Manulis and D. Pointcheval, "FlexibleGroup Key Exchange with On-demand Computation of Subgroup Keys," in Proc. Africacrypt 2010, 2010, vol. LNCS 6055, Lecture Notes in Computer Science, pp. 351-368.