**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 plaintext1. Hence, it is essential to find more flexible cryptographic primitives allowing dynamic broadcasts without a fully trusted dealer.

A. Our Contributions

We present the Contributory Broadcast Encryption (ConBE) primitive, which is a hybrid of GKA and BE. Compared to its preliminary Asiacrypt 2011 version [5], 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. Specifically, our main contributions are as follows. 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. Compared to BE, ConBE does not need a fully trusted third party to set up the system. 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. We observe that the aggregatability of AggBE schemes is necessary in the construction of our ConBE scheme and the BE schemes in the literature are not aggregatable. We construct a concrete AggBE scheme tightly proven to be fully collusion-resistant under the decision BDHE assumption. 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.

B. Potential Applications

A potential application of our ConBE is to secure data exchanged among friends via social networks. Since the Prism scandal [4], people are increasingly concerned about the protection of their personal data shared with their friends over social networks. Our ConBE can provide a feasible solution to this problem. Indeed, Phan et al. [6] underlined the applications of our ConBE [5] 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 can use our ConBE scheme. Since the setup procedure of our ConBE 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 instant messaging among family members, secure scientific

research tasks jointly conducted by scientists from different places, and disaster rescue using a mobile ad hoc network. A common feature of these scenarios is that a group of users would like to exchange sensitive data but a fully trusted third party is unavailable. Our ConBE provides an efficient solution

to these applications.