ABSTRACT

Broadcast encryption (BE) is an important cryptographic primitive whereby a broadcaster broadcasts an encrypted message (ciphertext) to a group of users over a public channel enabling only the users in the group to decrypt while the users outside the group are incapable of recovering the original message from the ciphertext. A BE scheme, in general, consists of a private key generation centre, a broadcaster and a group of users. The private key generation centre generates the common public parameter and secret keys for individual users. The broadcaster computes the ciphertext by encrypting a message and broadcasts it over a public channel. Each subscribed user recovers the message from the ciphertext using its own secret key issued by the private key generation centre through a secure communication channel between them in the offline phase prior to encryption and decryption. BE has numerous applications expanding from pay TV to digital right management. This thesis aims to construct secure and efficient BE variants of different flavours.

We have proposed two constructions of *broadcast encryption with dealership* (BED). In BED, a dealer selects a group of users and generates a group token hiding the group. A broadcaster publicly verifies the group size without knowing the group explicitly and generates the ciphertext from which each subscriber can recover the original message using its own secret key received over a secure communication channel from a private key generation centre. The existing work in this area is limited and requires considerable attention from the research community for developing new BED scheme due to its appealing numerous applications. In the existing BED construction of Gritti et al., the group token is not well binded, resulting, the dealer to cheat the broadcaster easily and thereby ruining broadcaster's business. Addressing the issue, we have designed two BED constructions in this thesis. One of our BED is selective secure in the random oracle model while the other provides adaptive security in the standard model.

Additionally, we have proposed two *recipient revocable broadcast encryption* (RRBE) schemes in the standard model. In RRBE, a broadcaster revokes a group of users from an encrypted content without being able to decrypt it. Our first RRBE construction achieves adaptive security whereas the second construction is selectively secure and computationally efficient when the number of revoked users are very few compared to the subscribed users.

We have also developed three constructions of *broadcast encryption with personalized messages* (BEPM) where a broadcaster broadcasts an encrypted common message together with encrypted personalized messages. On decryption, the common message can be recovered by all subscribed users while the personalize message

can be recovered by the individual subscribers to which message is intended. Our first construction in this field reduces the parameter sizes compared to Ohtake et al. and achieves selective security. More interestingly, our second construction achieves adaptive security. We have pointed out the constructional flaw in Xu et al. and proposed a BEPM construction with logarithmic parameter size using multilinear map.

Multi-channel broadcast encryption (MCBE) helps the broadcaster to send different encrypted broadcast messages to different groups of users utilizing only a single header containing encrypted information for recovering session keys for all the users in the system. Existing MCBE schemes are all in the private key setting and selectively secure. Our proposed constructions are in the public key setting. One of our construction achieves semi-static security while the other is selectively secure. Our selectively secure construction employs complete subtree method and provides outsider-anonymity by concealing the subscribed users' identity from the outsiders.

Keywords: broadcast encryption with dealership, recipient revocable broadcast encryption, broadcast encryption with personalized messages, multi-channel broadcast encryption, selective security, semi-static security, adaptive security, random oracle model, standard model, complete subtree method.