ABSTRACT

Broadcast Encryption (BE) allows secure transmission of encrypted data over an insecure public channel enabling only intended recipients to decrypt while outsiders recover nothing even if collude. Traditionally, a BE consists of three entities: a group manager, a broadcaster, and a group of users. The group manager first sets up the whole system by generating a master public-secret key pair. It also generates secret-keys for users and provides them in an offline phase. The broadcaster generates ciphertext corresponding to a message and a set of subscribers, making it publicly available. Each legitimate user belonging to the subscribers set recovers the correct message from the ciphertext by utilizing its secret-key. In contrast, the revoked users get nothing even if they collude. In this thesis, we design computationally efficient and secure public-key BE of different flavors with short communication bandwidth, optimal storage overhead and low computation cost.

Tracing systems empower a broadcaster to identify conspiracy of defrauders who collude to create a 'pirate decoder box' and revoke them. We propose construction for traceable BE in which broadcaster takes the revoked users set to generate the ciphertext. Our design is adaptive secure under the standard security model without q-type assumptions and random oracles.

Accomplishing the adaptive indistinguishable chosen-ciphertext attack security is still an open issue in the context of Private Linear Key Agreement (PLKA) whereby broadcaster takes a special linear type subscribers set to generate the ciphertext. Developing an efficient key encapsulation mechanism that provides both the functionalities of PLKA and traceability is a challenging task. We offer a solution to these problems and design a PLKA with compact parameter sizes which is fully collusion resistance and publicly traceabile without any security breach.

The outsider anonymity and public-key traceability are two mutually orthogonal properties of BE in terms of the subscribers' privacy. Although outsider anonymous BE and public-key traceable BE have been studied separately, it is hard to realize secure identity-based outsider anonymous public-key traceable BE without the efficiency degrade. We construct an identity-based outsider anonymous public-key traceable BE with proper security realization in standard security model without q-type assumptions and random oracles.

Achieving the adaptive security without q-type assumptions is still an open task in designing BE with Personalized Messages (BEPM) where a broadcaster transmits a common encrypted data together with encrypted personalized data. The existing BEPM do not provide adaptive security without q-type assumptions. Besides, they are unable to achieve anonymity of the recipients set. We propose adaptively secure identity-based anonymous BEPM that can support an exponential number of users without q-type assumptions and random oracles.

Existing Ciphertext-Policy Attribute-Based BE (CP-ABBE) are incapable of accomplishing full anonymity and privacy of access policy. To mitigate these issues, we design a fully anonymous adaptive CP-ABBE without q-type assumptions and random oracles in which the ciphertext-size is independent of access policy.

Keywords: broadcast encryption; traitor tracing and revoke; attribute-based encryption; identity-based encryption; anonymity; q-type security assumption; random oracle model.