Abstract

Broadcast Encryption (BE) is an advancement of the traditional cryptographic encryption mechanisms that ensures secure transmission of encrypted data over insecure public channels, allowing only intended recipients to decrypt the encrypted data while preventing outsiders from retrieving non-negligible information even if they collude. In a traditional BE setup, three primary entities are involved: a Private Key Generation Center (PKGC), a broadcaster, and a group of users, also known as the recipients. The PKGC initializes the system by generating a master public-secret key pair and distributing secret keys to users in an offline phase. The broadcaster then designs ciphertexts corresponding to messages and sets of subscribers, making them publicly available. Legitimate users in the subscribers' set can decrypt the messages using their secret keys, while illegitimate users receive negligible information about the original message even if they collude. In our thesis work, we focus on designing computationally efficient and robustly secure public-key BE schemes with short communication bandwidth, optimal storage overhead, and low computation costs to be suitable for resource-constrained devices.

Traceability in BE is crucial for identifying fraud conspiracies, such as the creation of 'pirate decoder boxes' and revoking offenders. Additionally, the BE with user anonymity has the property to hide information about subscribers from attackers. We address the challenge of achieving both the orthogonal properties, anonymity, and public-key traceability, in the BE framework, constructing an identity-based anonymous public-key trace and revoke system with robust security in the standard model without relying on q-type assumptions or random oracles.

Attaining adaptive security against chosen ciphertext attacks without q-type assumptions remains a challenging task in designing Broadcast Encryption with Personalized Messages (BEPM), where a broadcaster transmits common encrypted data alongside personalized encrypted data for individual subscribers. The existing BEPM protocols lack adaptive security without q-type assumptions and fail to ensure the anonymity of subscriber sets and the traceability of malicious users. To address this research gap, in this thesis, we propose an adaptively secure identity-based anonymous BEPM with traceability capable of supporting an exponential number of users without relying on q-type assumptions or non-standard random oracle model.

Due to recent advancements in quantum computing, existing number-theoretic assumptions-based BE protocols face certain vulnerabilities due to Shor's quantum algorithm. This thesis also develops quantum-safe BE protocols using multivariate quadratic polynomials, an emerging cryptographic tool for designing post-quantum encryption systems.

Keywords: Broadcast encryption; Traitor tracing and revoke; Identity-based encryption; Anonymity; q-type security assumption; Adaptive security; Random oracle model; Post-quantum security.

Ramprasad Sarkar