Abstract

Cryptosystems based on the attribute-based framework have recently acquired much importance due to their enhanced functionality and flexibility, and their promising potential as a cryptographic platform for achieving advanced functionalities. However, attribute-based cryptosystems incur high communication and computation overheads which could impede their practical usage. This thesis aims at designing efficient and provably secure attribute-based cryptographic schemes allowing for expressive access policies with significantly low communication and computation cost, using bilinear pairings.

The contributions of the thesis are manifold. We first propose two Key-Policy Attribute-Based Encryption (KP-ABE) schemes with constant-size ciphertext for Linear Secret-Sharing Scheme (LSSS)-realizable (monotone) access structures, supporting small universes of attributes. Among these, one scheme is Chosen Plaintext Attack (CPA) secure and the other is chosen ciphertext attack secure. We then extend these schemes to support not only the positive but also the negative attributes. Next, a CPA secure KP-ABE for large attribute universes is presented that features linear-size ciphertext and constant-size public parameters. Later, a dual-policy ABE with short ciphertext and constant-size ciphertext broadcast KP-ABE schemes are constructed.

In all the aforementioned schemes, one fully trusted authority manages attributes and issues secret decryption keys to legitimate users. We suggest a decentralized multi-authority Ciphertext-Policy ABE (dCP-ABE) for general monotone access structures. We incorporate the ciphertext access control policy in terms of minimal authorized sets in access structure, without using any secret-sharing scheme.

Further, we present a key-policy Attribute-Based Signature (ABS) with constant-size signature and an Attribute-Based Signcryption (ABSC) with constant-size ciphertext for LSSS-realizable access structures. Both the schemes can preserve signer privacy. In addition, our ABSC achieves public verifiability of the ciphertext, enabling any party to verify the integrity and validity of the ciphertext. Finally, we introduce key-insulated mechanism with message recovery in ABS scenario and present two key-policy attribute-based key-insulated signature schemes with message recovery. The first scheme deals with small universes of attributes while the second scheme can work for large attribute universes.

All the proposed schemes, except dCP-ABE, are provably secure in selective security model under decisional Bilinear Diffie-Hellman Exponent or computational Diffie-Hellman Exponent assumptions. The security of dCP-ABE is argued in

generic bilinear group assumption. The secret key (decryption key or signing key) size in all the proposed constructions (except in dCP-ABE) is quadratic in number of involved attributes. However, the number of required bilinear pairing evaluations is constant, that is, independent of the number of underlying attributes.

Keywords: attribute-based cryptography, attribute-based encryption, attribute-based signature and signcryption, bilinear pairing, ciphertext-policy, constant-size, dual-policy, key-policy, key-insulation mechanism, linear-secret sharing scheme, multi-authority, message recovery, monotone access structure, non-monotone access structure, selective security.