Abstract

Nowadays, the convergence of Internet of Things (IoT) and cloud computing is facilitating global accessibility, scalability, innovation and virtualization. The IoT devices collect a vast amount of sensitive data and untrusted cloud server stores as well as processes this data with emerging applications in big-data analysis, e-commerce, accounting, and management. Although this paradigm offers numerous benefits, there are issues of data breaches, unauthorized access, and privacy leakage. To resolve this issues, traditional *public key encryption* (PKE) has been refined over the years into more sophisticated method of encryption like *Identity-based encryption* (IBE), *Attribute-based encryption* (ABE), *Broadcast encryption* (BE), and *Functional encryption* (FE). These advanced primitives monitor fine-grained access control of sensitive data in untrusted cloud environment. This thesis mainly aims to design variants of advanced encryption techniques. All the proposed schemes are provably secure based on pairing-based assumptions.

We propose the first *hierarchical identity-based inner product functional encryption* (HID-IPFE) based on a standard assumption. Previously, there was HID-IPFE based on a stronger q-type assumption. We also extend the notion of HID-IPFE that supports unbounded hierarchical depth and we call it *unbounded* HID-IPFE (UHID-IPFE). This is suitable for practical deployment as it does not fix the maximum hierarchy depth at the Setup phase. We present UHID-IPFE which achieves better storage compared to the previous schemes. Both our HID-IPFE and UHID-IPFE achieve selective security in the standard model and the underlying group in these schemes is of prime order. We also present a *key-policy attribute-based inner product functional encryption* (KP-ABIPFE) based on three subgroup decisional problems in a composite order bilinear group. Our KP-ABIPFE achieves adaptive security in the standard model.

We construct two *revocable ciphertext-policy attribute-based key encapsulation mechanism* (RCP-ABKEM) designs satisfying key-homomorphic property. Our schemes are the first to achieve revocability and key-homomorphic property concurrently in an attribute-based setting. Our first protocol achieves selective security in the standard model and this setting is bilinear. Our second protocol is proved to be selectively secure in the random oracle model and this setup is multilinear. As a refined primitive, our proposed key-homomorphic RCP-ABKEM is of independent interest and may be utilized as a building block for designing privacy-preserving protocols.

We introduce the notion of *certificateless inner product broadcast encryption*

(CL-IPBE) to fix the issues of key-escrow and certificate management from the setting and enable inner product computation on encrypted data. Previously, there was a concept of *certificate-based inner product broadcast encryption* (CB-IPBE). This setting makes use of certificate. We aim to resolve this utilizing certificateless setting. We provide instantiation of CL-IPBE based on standard assumption. Our design achieves indistinguishability and anonymity against two types of adversary – Type-1 and Type-2. The security proofs of our protocol follow the standard model. Furthermore, our design offers better storage compared to the previous CB-IPBE design.

Trapdoor function (TDF) serves as mathematical foundation in all the PKE schemes. It is a mathematical function that is easy to compute in one direction but hard to reverse without the special information called trapdoor. *Threshold trapdoor function* (TTDF) is a variant of TDF in threshold setting. It enables sharing the master trapdoor among different servers so that at least a threshold number of servers jointly can revert, but the number of servers below the threshold cannot. There is an existing construction of TTDF based on standard assumption. We provide a concrete instantiation of TTDF based on a weaker assumption. Our design achieves one-wayness despite the compromise of a certain subset of servers. Moreover, our design performs better regarding communication bandwidth.

Keywords: hierarchical identity, inner product functional encryption, unbounded depth, attribute-based encryption, key-policy, ciphertext-policy, key-encapsulation mechanism, revocation, key-homomorphism, broadcast encryption, certificateless setting, Shamir's threshold secret sharing.