Abstract

Functional encryption (FE) has emerged as a powerful tool in the realm of cloud computing, offering enhanced security and privacy for outsourced data processing. This thesis explores the application of FE in cloud computing environments, highlighting its efficacy in ensuring data confidentiality while enabling selective access to encrypted data depending on attribute-based *linear* functions. We delve into the theoretical underpinnings of FE and discuss its practical implications for cloud-based applications, including secure data sharing, fine-grained access control, privacy-preserving computation, and traceability. The objective of the thesis is to design and analyze more advanced cryptographic primitives for linear functions, namely *inner product encryption* (IPE), *predicate inner product functional encryption* (P-IPFE) with a practically sound *unbounded* feature, and *traceable* FE scheme for *identity-based inner product* FE (IBIPFE), which enhance security and privacy in cloud computing infrastructures. The feature of unboundedness expands the applicability of the primitives in scenarios where the length of vectors varies or is not known in advance. Additionally, the traceability property ensures the identification of dishonest users (traitors) who embed their secret keys into a pirate decoder to decrypt unauthorized ciphertexts, thus preventing significant losses to content providers. More precisely, the contributions are outlined as follows:

We construct an efficient *adaptive fully attribute-hiding* (AD-FAH) secure *unbounded zero* IPE (UZIPE) scheme under the *symmetric external Diffie-Hellman* (SXDH) assumption. Concretely, it provides indistinguishability-based security in the standard model. Our UZIPE enjoys short secret keys and ciphertexts, which reduce storage and communication costs.

We present the *first* concrete construction of *payload-hiding* secure *unbounded non-zero* IPE (UNIPE) based on the SXDH assumption in the standard model. Additionally, we propose a generic construction of UNIPE from *unbounded inner product* FE (UIPFE) with *weak attribute-hiding* security. Furthermore, we present an instantiation of the *adaptive weak attribute-hiding* (AD-WAH) secure UNIPE based on the SXDH assumption. We exhibit applications of attribute-hiding UNIPE in designing an *unbounded anonymous identity-based revocation* (UAnon-IBRV) scheme. Here, the size of the revoke users set is unbounded and chosen at the time of key generation.

Next, we introduce a primitive called *unbounded attribute-based* IPFE (UABIPFE), allowing users to encrypt messages of unbounded length along with an arbitrary number of hidden attributes into ciphertexts. We define a subclass of UABIPFE called *unbounded zero predicate* IPFE (UZP-IPFE), which is designed for both *public* and *secret* key settings. Initially, we design the *first public* key UZP-IPFE, which hides unbounded sizes of *attributes* associated with ciphertexts and achieves the *semi-adaptive full attribute-hiding* (SA-FAH) security in the indistinguishability-based model under the SXDH assumption. Furthermore, we present the *first secret* key UZP-IPFE, referred to as *secure access control in* FE (SACfe), which achieves *semi-adaptive full-hiding* (SA-FH) security based on the SXDH assumption. This SA-FH feature ensures that both the user-specific information (i.e., attributes and functions) are hidden in the ciphertext and secret keys.

We embark on an exploration of *unbounded non-zero predicate* IPFE (UNP-IPFE), a specific subclass of UABIPFE, delving into its characteristics and applications. We generically transform an *unbounded quadratic* FE (UQFE) scheme and UIPFE into a *weak attribute-hiding* UNP-IPFE against *semi-adaptive* adversaries in both *secret* and *public* key settings: (a) we present the *first secret* key simulation-secure UNP-IPFE with *succinct* secret keys, constructed from a novel *succinct* UQFE designed in the random oracle model (ROM) based on the *bilateral k-lin* assumption (b) we present a *public* key UNP-IPFE derived from UQFE and UIPFE, achieving *weak attribute-hiding* indistinguishability-based security against *semi-adaptive* adversaries in ROM.

We introduce the *embedded identity* TIBIPFE (EI-TIBIPFE), the *first fully collusion-resistant* and *traceable identity-based* IPFE (TIBIPFE) scheme. This scheme directly traces traitors' identities via an efficient tracing mechanism. Our approach involves a generic construction of EI-TIBIPFE from an intermediate primitive known as *embedded identity private linear* IBIPFE (EIPL-IBIPFE). Furthermore, we demonstrate the construction of a *selectively* secure EIPL-IBIPFE from the *decisional 3-party Diffie-Hellman* (D3DH) assumption in the standard model.

Keywords. cloud computing, unbounded, attribute-hiding, payload-hiding, inner product encryption, functional encryption, inner product functional encryption, predicate inner product functional encryption, adaptive security, semi-adaptive security, selective security.