ABSTRACT

This thesis presents *better* constructions of *functional encryption* (FE) for *inner products* and (*revocable*) *attribute-based encryption* (ABE), introduces the notion of *functional signcryption* (FSC) together with a concrete FSC scheme, and designs *improved* (*verifiable*) *constrained pseudorandom function* (CPRF). We precisely make the following contributions:

- We present the *first non-generic* and *simple* FE scheme for inner products, achieving the *full-hiding* security in its *strongest* form. The construction is built in *prime* order bilinear group, under the *Symmetric External Diffie-Hellman* assumption.

- We design a selectively secure ABE scheme for *arbitrary polynomial-size circuits*, featuring *short* ciphertexts and *shorter* decryption keys compared to the existing similar constructions. We further present two selectively secure *directly* revocable ABE (RABE) schemes which are the *first* to support *general circuits* and *constant* number of revocation controlling components within ciphertexts and decryption keys. The public parameter size in our first RABE construction is *linear* to the maximum supported number of decrypters, while in our second construction we reduce it to *logarithmic*. Our ABE and RABE constructions are developed using multilinear maps, under *standard* complexity assumptions.

- We propose a *new* cryptographic primitive, termed as *functional signcryption* (FSC), that *unifies* the functionalities of both FE and FS into a *cost-effective* formulation. We also present an instantiation of FSC that supports *arbitrary polynomial-size circuits*, based on *indistinguishability obfuscation* (IO). We further exhibit some representative applications of FSC.

- In EUROCRYPT 2016, Deshpande et al. presented a CPRF construction supporting inputs of *unconstrained polynomial length*, based on IO. We demonstrate that contrary to their claim, the proposed CPRF actually achieves security not in the selective model, rather in a *significantly weaker* model where the adversary is forbidden to query constrained keys adaptively. We show how to allow *adaptive* constrained key queries in their construction. We propose an improved CPRF by carefully modifying their construction without any additional heavy-duty tool, and redesign the security proof. Our CPRF is further enhanced to present the *first* construction of *constrained verifiable pseudorandom function* (CVPRF) supporting inputs of *unconstrained polynomial length*, employing only standard public key encryption.

Keywords: functional encryption, inner product, full-hiding security, attribute-based encryption, general polynomial-size circuits, revocation, functional signcryption, constrained pseudorandom function, constrained verifiable pseudorandom function, Turing machines, bilinear maps, multilinear maps, indistinguishability obfuscation