ABSTRACT

Most of the modern public key cryptosystems in use today are based on either integer factorization problem or discrete logarithm problem. In 1999, Peter Shor showed that quantum computers can break such number theoretic problems in polynomial time. With the growing interest in quantum technology, it is necessary to find post-quantum alternatives to the classical public key cryptosystems based on mathematical problems that are not affected by an attacker equipped with a quantum computer. Among the variants of Post-Quantum Cryptography (PQC), lattice-based cryptography attracts lots of attention as they have flexible structure, algorithmically simple, efficient and highly parallelizable. Fully Homomorphic Encryption (FHE) is an advanced primitive based on the lattices which has several practical applications including cloud computing. Multi-key FHE in a dynamic setting is the most versatile variant of FHE which requires no information about the participating parties prior to key generation. Designing dynamic multi-key FHE without blowing up the storage and ciphertext size of homomorphic computation is a challenging task. In this thesis, we propose a dynamic (leveled) multi-key FHE scheme under the Learning With Errors (LWE) assumption. Unlike the existing LWE based multi-key FHE, our design does not use any common reference matrix in the common parameter which strengthens the power of using multi-key FHE as it allows users to generate their own keys independently.

Furthermore, we presented a multi-key FHE that can encrypt multi-bit messages with non-interactive decryption and chosen-plaintext attack (IND-CPA) security under LWE assumption. Apart from efficient homomorphic addition and multiplication, our technique of extending a ciphertext under additional keys yields significant reduction in the computational overhead. When contrasted with the existing multi-key FHE schemes for multi-bit messages, our candidate exhibits favorable results in the length of the secret key, public key and ciphertext preserving non-interactive decryption.

We also design an Enhanced Privacy ID (EPID) signature scheme based on lattices which is, to the best of our knowledge, the first post-quantum variant of EPID signature with security under the hardness of the Short Integer Solution (SIS) problem. Our construction employs an updatable Merkle tree accumulator which provides flexibility to our EPID signature by allowing dynamic joining or revoking of any group members at any time. We provide an estimated efficiency comparison of our EPID signature with the existing similar schemes which shows that our scheme is efficient and enjoys post-quantum security.

Besides lattice-based cryptography, Multivariate Public-Key Cryptosystem (MPKC) is another promising PQC candidate due to its high computation speed and decent computational resource requisite, making it suitable for resource-constrained devices like Radio Frequency Identifications (RFIDs) or smart cards. In the last two decades, there has been remarkable development in MPKC, especially in signature schemes. In this thesis, we concentrate on designing a secure and efficient multivariate Identity-Based Signature (IBS) scheme with concrete security analysis in the existing security models. Integrating a specialized version of non-interactive zero-knowledge proofs of knowledge, called the signature of knowledge, we develop an multivariate identity-based signature scheme, namely MV-IBS. We emphasize that unlike most of the MPKC schemes in the literature which claim their security either heuristically or experimentally, our construction is existentially unforgeable against chosen message and chosen identity attack (EUF-CMA) in the Random Oracle Model (ROM) under the hardness of the Isomorphism of Polynomials (IP) problem. Moreover, our proposed MV-IBS performs significantly better over the existing MPKC based IBS in terms of the master secret key size, master public key size and user secret key size.

Additionally, we employ a code-based approach and design a new method for Key Predistribution Scheme (KPS) by building a communication model and a connectivity model. We exploit the Reed Solomon code to establish our communication model, integrate the binary Goppa code to derive our connectivity model and skillfully blend these two models to construct our code-based KPS. An implementation in C language confirms the significant performance gain of our KPS over the existing similar works.

Keywords: post quantum cryptography, lattice based cryptosystem, multi-key fully homomorphic encryption, learning with errors, multi-bit messages, lattice-based signature, Unforgeability, Anonymous attestation, identity based signature, isomorphism of polynomials problem, signature of knowledge, EUF-CMA security, Goppa codes, Reed Solomon codes, connectivity key, communication key.