Abstract

Due to the extensive use of advanced and smart technology worldwide, designing robust, secure and cost-effective primitives become necessary to fulfill the rising demand for security in advanced computational scenarios. The security of cryptosystems developed on number-theoretic assumptions will be in doubt as soon as powerful fault tolerant quantum computers are a reality. Post-quantum cryptography guarantees secure primitives in the presence of computers equipped with quantum computing. Error-correcting codes and multivariate polynomials play significant roles in designing cryptographic techniques to ensure safety in communicating information against quantum attackers. In this thesis, we explore quantum-safe cryptographic primitives using error-correcting codes and multivariate polynomials and design key encapsulation mechanism (KEM) preserving data privacy, group signature scheme exhibiting anonymity, non-frameability, traceability, tracing-soundness and deniability feature and attribute-based signature (ABS) scheme with unforgeability and perfect privacy for fine-grained control over signing attribute information.

KEM is an essential building block in cryptography that is vital in transmitting symmetric key information securely utilizing asymmetric algorithms. We present two promising KEM constructions based on two different error-correcting codes which are secure against indistinguishability under chosen ciphertext attacks (IND-CCA) in the random oracle model under the hardness of generic decoding problem. Our first KEM employs the dyadic form of the parity check matrix of the Generalized Srivastava code. The scheme is an improvement over an existing KEM based on Generalized Srivastava code in terms of communication bandwidth. Our second KEM is storage-friendly and designed from maximum distance separable (MDS) codes employing a simple-but-insightful trick to utilize a companion matrix. When contrasted to other existing similar approaches, our KEM exhibits better performance guarantee in terms of ciphertext and secret key size.

Studying group signature has been one of the most versatile areas of cryptographic research having multiple applications to data privacy and security. Group signature allows members of a group to sign a document on behalf of the group while maintaining the signer's anonymity and enabling the revelation of the signer's identity in required circumstances. We introduce the *first* fully-dynamic code-based group signature scheme that allows group members to join or leave anytime. We skillfully incorporate a secure code-based Merkle-tree accumulator based on a collision-resistant code-based hash function, hire the double encryption technique to a randomized variant of the Niederreiter encryption that relies on binary Goppa code and combine it with a Stern-like zero-knowledge argument of knowledge. Moreover, we added deniability feature to our system so that the tracing authority may provide proof that a specific member did not sign a particular signature. More interestingly, our protocol performs favourably in terms of group public key size, secret key size and signature size compared to the existing code-based group signature schemes. Our scheme features anonymity, non-frameability, traceability and tracing-soundness in the random oracle model under the hardness of generic decoding problem.

The future of digital safety in post-quantum era seems promising with the adoption of multivariate public key cryptosystems (MPKC) even against quantum adversaries. MPKCs derive their security from the fact that solving a random system of multivariate polynomial equations over a finite field is an NP-hard problem. We provide an in-depth analysis of multivariate public key encryption and signature schemes, specifically targeting security, efficiency and parameter choice. We begin with a brief introduction to state of the art in security threats covering topics like MinRank attack, differential attack, finding a Gröbner basis for a direct attack etc. Besides, it covers the algorithms that are required for implementing multivariate schemes. We also provide a comparative study on promising multivariate encryption and signature schemes.

With the rapid evolution of computer networks, more and more messages are exposed in an open environment. Hence, protecting user's signing attribute information is crucial to mitigate the risk of unauthorized access. ABS scheme is an important cryptographic primitive for safeguarding the privacy of user's signing attribute information. We integrate salted-UOV and the 3-pass identification scheme and present the *first* ABS scheme in multivariate quadratic (MQ) setting. Our candidate utilizes an approach by representing the policy as a monotone span program. Moreover, our proposal provides adaptive predicate existential unforgeability under chosen message attack in the random oracle model. It also supports perfect privacy which ensures that a signature cannot be linked to the set of attributes or the secret signing key that generated the signature. Moreover, our scheme provides a significant advantage regarding signature size and signing key size compared to the existing post-quantum ABS schemes.

Keywords: Post-quantum cryptography, Key encapsulation mechanism, Group signature, Attribute-based signature, Generalized Srivastava code, MDS code, Goppa code, Companion matrix, Merkle-tree, Syndrome decoding problem, Multivariate polynomials, MQ problem