ABSTRACT

Digital signatures play an extremely important role in software updates, online payments, e-banking, e-commerce, etc. It is considered to be the most important tool to provide authentication of a message and achieve information security. In the current era, most of the digital transactions use digital signatures that are publicly verifiable and they bind the signatory to the message. The privacy of signatures is a very sensitive and generic concept due to which different types of signatures have been evolved. Based on various situations and scenarios, many schemes have been proposed in the literature. In general, privacy providing signatures can be classified on the basis that they protect signers identity from being revealed to unauthorized parties which are not associated with it, or they make the signed message to pre-designated parties private. Various types of non-transferable signatures are available and some of them are undeniable signatures, designated verifier signatures, chameleon signatures, nominative signatures, universally designated verifier signatures, etc.

The majority non-transferrable signatures are constructed based on the hardness of discrete logarithm problem and integer factorization problem. However, these problems could be solved in polynomial time by quantum computer (Shor 1994). Hence, it is of utmost importance to develop non-transferable signatures which remain secure even when the adversary has access to a quantum computer. In an attempt to address this problem, this research proposes non-transferable signature schemes that are secure and safe to quantum attacks.

Hash-based signature schemes are considered as an efficient replacement to those schemes that are vulnerable to quantum computer attacks. One of the primary advantages in the construction of this scheme is that it does not require any specific complex algebraic structures and mathematical operations, but has very minimal requirements such as the existence of cryptographic hash functions. These functions ensure the integrity of the data and also take care of infrastructures such as encryption, key management, secure web-connections, password logins, virus and malware-scanning and digital signatures. One of the biggest advantages of the construction of the hash-based signature scheme is that, the underlying hash functions can be chosen based on the availability of hardware and software resources. This signifies that the hash function can be replaced by another hash function if an attack is performed on it, without making any changes to the overall construction or structure of the scheme. Also, the security of the signature scheme can be validated by providing basic proofs of security reductions to the property of hash function. Significant research is conducted on the design and development of privacy preserving hash-based signatures.

Apart from these hash-based signatures, there is a promising alternative to classical digital signatures called code-based signatures. These signatures are very secure towards classical and quantum attacks. The code-based signatures includes efficient executable simple operations and are very fast compared to others. They come up with many strong features in addition to being secure from quantum attacks. The signature generation and the verification processes are very quick and easy to implement compared to other number-theoretic based signature schemes as the operations involved are only matrix-vector multiplications. Therefore, it is considered to be a viable choice to design code-based signature schemes.

This research investigates the approaches for designing non-transferable signatures that are required for some real-time scenarios and extends hash-based and code-based ordinary signature schemes that are immune to classical and quantum attacks to digital signature schemes with additional properties that could render non-transferable signatures. It also provides construction of various hash-based and code-based non-transferable signature schemes.

The first four Chapters of this dissertation present an overall introduction, the construction of undeniable signature scheme, chameleon signature scheme and designated verifier signature scheme based on one-way functions with additional homomorphic property. The design of the schemes uses only cryptographic hash functions and pseudorandom generator instead of using a specific algebraic structures having trapdoors. These works also investigate the security of the schemes and provide security reduction proofs to the hash function properties in the random oracle model. The following Chapters present the construction of designated verifier signature, chameleon signature and a variant of universal designated verifier signature based on the hard problems in coding theory that are believed to be secure against quantum attacks. In the fifth Chapter, the vulnerabilities in the recently proposed code-based Designated Verifier Signature (DVS) schemes by Ren *et al.* (2016) and Shooshtari *et al.* (2016) are identified and a new code-based one-time DVS is designed that overcomes the identified vulnerabilities. The unforgeability in the random oracle model is also proved. A comparative analysis of the performance of the proposed scheme is done with that of the existing code-based DVS schemes and it is observed that the proposed scheme is fast particularly in the signature generation process. In the next Chapter, a code-based chameleon hashing and signature scheme with the security requirements of the chameleon hash function such as collision resistance, semantic security and key exposure freeness is developed. In addition, a publicly verifiable signature scheme is

constructed from the chameleon hash function and its unforgeability in random oracle is proved. A comparative analysis of the performance of the proposed scheme is done with that of the existing chameleon signature schemes. The last Chapter presents a code-based universal designated verifier signature proof based on syndrome decoding problem that could render a promising alternative to the existing universal designated verifier signature systems that are immune to quantum attacks.