AN INVESTIGATION AND DESIGN OF POST-QUANTUM PRIVACY PRESERVING SIGNATURES

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. As an ordinary digital signature is universally verifiable, it undesirable for those applications that are personally or commercially sensitive. In many applications such as e-voting, e-commerce, etc., privacy providing signatures are required. Non-transferable signatures are also called as private signatures that enable the signer or the recipient to decide who can verify the issued signature. 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. Majority of the non-transferrable signatures are constructed based on the hardness of discrete logarithm problems and integer factorization problem.However, these problems could be solved in polynomial time by quantum (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 required for some real-time scenarios and are secure and safe to quantum attacks. The research 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.