**ABSTRACT**

In today’s world, digital signatures are an indispensable element for secured communication applications. They are needed, to ensure the authentication of a communication partner, i.e. in web services like Email or chats. They are also needed, to ensure the authentication of a web server for web services like web-shops or online-banking. But digital signatures are not just used in web services. For example, they can also be used to verify the validity of digital passports or other digital documents.

Popular signature schemes are the Digital Signature Scheme (DSA) and the RSA Signature Scheme. The security of these schemes relies on the difficulties of solving the discrete logarithm problem and the problem of factorizing large numbers. Today, no efficient algorithms are known to solve these problems, so that these schemes are considered secure. However, it is not proven that no such algorithms exist. If the mathematicians are able to find a suitable algorithm, these signature schemes would become insecure. Furthermore, there are already algorithms known to solve these problems in case a quantum computer can be build. Some scientists believe it might be possible to build a quantum computer in about 20 years. Therefore, alternative digital signature schemes are needed, in case the signature schemes based on the discrete logarithm problem or the factorization problem become insecure.

Merkle tree traversal technique is introduced for the same. It begins with the original tree traversal and then two improvements. Although hash functions are very efficient, too many secret leaf values would need to be authenticated for each digital signature. By reducing the time or space cost, we found that for medium - size trees the computational cost can be made sufficiently efficient for practical use. This reinforced the belief that practical, secure signature/authentication protocols are realizable, even if the number theoretic algorithms were not available.