

Abstract

With more and more research focusing on Health Care services, there is need for efficient authentication by use of digital signatures. Currently, the DSA is one of the most commonly used digital signature scheme. This paper proposes an Optimized Health Batch Verification Scheme on a variant of DSA. The proposed system is based on a new optimal DSA-type digital signature scheme, which is also proposed in this paper. Our scheme makes use of Small Exponents Test and Bucket Test subroutines for optimization. Performance evaluation shows that our scheme is significantly more efficient in batch verification of digital signatures, making it suitable for Health applications. The Scheme is secure against authentication threats, message integrity threats and replay attack threats.