Abstract

With the current developments in wireless networks, the use of Wireless sensor networks (WSNs) in the medical field has attracted a lot of attention. WSNs are being used to collect and transmit patient physiological information in ubiquitous healthcare systems. One of the major challenges in healthcare systems is security and privacy of patients' vital data. By its very nature, a wireless sensor network provides a resource constrained environment and sensor nodes used in WSNs are limited in terms resource usage. Keeping data secure in a resource constraint environment is an important and challenging task. Hence, the need for secure and more efficient cryptosystems. In this paper, we are proposing a secure pairing-free certificateless signcryption scheme for use in ubiquitous healthcare systems. We compare the efficiency of our proposed scheme with other related signcryption schemes. A formal security proof for indistinguishability against adaptive chosen ciphertext attack and unforgeability against adaptive chosen message attack for our scheme is presented in random oracle model.