DOI: 10.24178/ijsms.2018.3.1.07

Algebraic Verification Algorithm

Areej M. Abduldaim
Department of Applied Sciences
University of Technology
Baghdad, Iraq
areejmussab@gmail.com

***Abstract*—Authentication over insecure public networks or with untrusted servers raises more concerns in privacy and security.Modern algebra is one of the significant fields of mathematics. It is a combination of techniques used for a variety of applications including the process of the manipulation of the mathematical categories. In addition, modern algebra deals in depth with the study of abstractions such as groups, rings and fields,the main objective of this article is to provide a novel algebraic verification protocol using ring theory. The protocol is blind, meaning that it detects only the identity, and no additional information will be known anything about the prover (the biometric) to the authenticating server or vice-versa. More officially a blind authentication scheme is a cryptographic protocol that comprises of two parties, a user (the prover) that wants to achieve having signs on her messages, and a signer (the verifier) that is in ownership of his secret signing key. In this paper, we employ the algebraic structure called central Armendariz rings to design a neoteric algorithm for zero knowledge proof. The proposed protocol is established and illustrated through numerical example, and its soundness and completeness are proved. This method gave two important properties for the central Armendariz zero knowledge protocol compared with other known protocols.**

***Keywords*—Central Armendariz rings, Authentication, Zero Knowledge Protocol, Cryptography, Polynomial Ring**