World Academy of Science, Engineering and Technology
International Journal of Physical and Mathematical Sciences
Vol:11, No:09, 2017

Generalized π-Armendariz Authentication Cryptosystem

Authors : Areej M. Abduldaim, Nadia M. G. Al-Saidi

Abstract : Algebra is one of the important fields of mathematics. It concerns with the study and manipulation of mathematical symbols. It also concerns with the study of abstractions such as groups, rings, and fields. Due to the development of these abstractions, it is extended to consider other structures, such as vectors, matrices, and polynomials, which are non-numerical objects. Computer algebra is the implementation of algebraic methods as algorithms and computer programs. Recently, many algebraic cryptosystem protocols are based on non-commutative algebraic structures, such as authentication, key exchange, and encryption-decryption processes are adopted. Cryptography is the science that aimed at sending the information through public channels in such a way that only an authorized recipient can read it. Ring theory is the most attractive category of algebra in the area of cryptography. In this paper, we employ the algebraic structure called skew -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.

Keywords : cryptosystem, identification, skew π-Armendariz rings, skew polynomial rings, zero knowledge protocol
Conference Title : ICMMS 2017 : International Conference on Mathematics and Mathematical Sciences
Conference Location : Paris, France
Conference Dates : September 21-22, 2017