2nd International Conference on Applied Research in
ENGINEERING SCIENCE & TECHNOLOGY
18-20 October 2019 Budapest, Hungary

A Novel Public Key Cryptosystem and Digital Signatures

Saba Inam[1, *], Shamsa Kanwal[1], Adnan Zahid[2], Maria Abid[1]

[1] Fatima Jinnah Women University, The Mall, Rawalpindi, Pakistan [2]Quaid-i-Azam University, Islamabad, Pakistan

Abstract.

In this article, we develop a new algebraic public key cryptosystem, which is based on generally non-commutative ring. Firstly, we define the polynomials over the non-commutative rings and then take it as underlying work structure. The hard problem of the scheme is the mixture of matrix discrete log problem under modular classes and polynomial symmetric decomposition problem. Using matrices of higher order and large modular classes resist the brute force and other well-known attacks exists in the literature. We also discuss the computational complexity of proposed scheme. On the other hand, we propose a signature scheme over a non-commutative division semiring. The key idea behind the signature scheme is that, for a given noncommutative division semiring, we build a polynomial and then implement digital signatures on multiplicative structure of semiring.

Keywords: Hash Function, Signature Scheme, Key Exchange Protocol, Complexity.