International J. of Math. Sci. & Engg. Appls. (IJMSEA)
ISSN 0973-9424, Vol. 7 No. II (March, 2013), pp. 371-383

SECURED DIRECTED DIGITAL SIGNATURE SCHEME USING POLYNOMIAL OVER NON-COMMUTATIVE GROUPS

G. S. G. N. ANJANEYULU[1], V. MADHU VISWANTHAM[2] AND A. VIJAYABARATHI[3]

[1] Associate professor, Applied Algebra Division,
School of Advanced Sciences, VIT University, Vellore-14, Tamilnadu, India
[2] Associate professor, School of Computing Science
and Engineering, VIT University, Vellore-14, Tamilnadu, India
[3] Research Scholar, Applied Algebra Division,
School of Advanced Sciences, VIT University, Vellore-14, Tamilnadu, India

Abstract

Directed digital signatures are probably the most important and widely used cryptographic primitive enabled by public key technology, and they are building blocks of many modern distributed computer applications. But many existing signatures schemes lie in the intractability of problems closely related to the number theory than group theory. In this paper, we would like to propose new technique for directed digital signature scheme based on general non-commutative groups. The key idea of our proposal is that for given non-commutative group and using monomorphism, we select polynomials and we construct all digital scheme parameters on groups using monomorphism. This monomorphism can be used in all calculations of parameters of signature scheme. The security of the proposed directed signature scheme and registration number is based on the intractability of the Polynomial Symmetrical Decomposition Problem over the given non-commutative division semirings.

Key Words : *Directed Digital Signature, Polynomial Decomposition problem, Non-commutative Division Semi ring, Registration number.*