A PUBLIC–KEY CRYPTOSYSTEM BASED ON RÉDEI RATIONAL FUNCTIONS AND CONICS

NADIR MURRU

ABSTRACT. We use an irreducible polynomial of degree 2 to define a quotient field that induces a product over certain conics. This product gives conics a group structure. By means of a convenient parametrization, we define a group structure over the set of parameters, where powers are performed by rational polynomials evaluated by means of Rédei rational functions. We prove that, in special cases, these groups have finite order and consequently we can construct a novel public–key cryptosystem. The use of rational polynomials in the encryption algorithm shows a significant difference with respect to classical RSA scheme.

RESEARCH FELLOW, UNIVERSITY OF TURIN, ITALY
E-mail address: nadir.murru@unito.it