CORR 2000-49

New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups

S.S. Magliveras*, D.R. Stinson, & Tran van Trung*

Abstract A symmetric key cryptosystem based on *logarithmic signatures* for finite permutation groups was described by the first author in [6], and its algebraic properties were studied in [7]. In this paper we describe two possible approaches to the construction of new public key cryptosystems with message space a large finite group G, using logarithmic signatures and their generalizations. The first approach relies on the fact that permutations of the message space G induced by transversal logarithmic signatures almost always generate the full symmetric group S_G on the message space. The second approach could potentially lead to new ElGamal - like systems based on trap-door, one-way functions induced by logarithmic signature-like objects we call *meshes*, which are *uniform covers* for G.

Keywords Trap-door one-way functions, group factorizations, public key cryptosystems, finite groups.