Mahalanobis, Ayan
The MOR cryptosystem and extra-special $p$-groups. (English) Zbl 1495.94059

Summary: This paper studies the MOR cryptosystem, using the automorphism group of the extra-special $p$-group of exponent $p$, for an odd prime $p$. Similar results can be obtained for extra-special $p$-groups of exponent $p^2$ and for the even prime.

MSC:
94A60 Cryptography
20D15 Finite nilpotent groups, $p$-groups
20D45 Automorphisms of abstract finite groups

Keywords:
MOR cryptosystem; extra-special $p$-groups; discrete logarithm problem

Full Text: DOI arXiv

References:

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.