World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:17, No:06, 2023

A Generalization of the Secret Sharing Scheme Codes Over Certain Ring

Authors : Ibrahim Özbek, Erdoğan Mehmet Özkan

Abstract : In this study, we generalize (k,n) threshold secret sharing scheme on the study Ozbek and Siap to the codes over the ring Fq+ αFq. In this way, it is mentioned that the method obtained in that article can also be used on codes over rings, and new advantages to be obtained. The method of securely sharing the key in cryptography, which Shamir first systematized and Massey carried over to codes, became usable for all error-correcting codes. The firewall of this scheme is based on the hardness of the syndrome decoding problem. Also, an open study area is left for those working for other rings and code classes. All codes that correct errors with this method have been the working area of this method.

Keywords : secret sharing scheme, linear codes, algebra, finite rings
Conference Title : ICACA 2023 : International Conference on Advanced Commutative Algebras
Conference Location : San Francisco, United States
Conference Dates : June 05-06, 2023