World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:9, No:10, 2015

Comparison between Separable and Irreducible Goppa Code in McEliece Cryptosystem

Authors : Newroz Nooralddin Abdulrazaq, Thuraya Mahmood Qaradaghi

Abstract : The McEliece cryptosystem is an asymmetric type of cryptography based on error correction code. The classical McEliece used irreducible binary Goppa code which considered unbreakable until now especially with parameter [1024, 524, and 101], but it is suffering from large public key matrix which leads to be difficult to be used practically. In this work Irreducible and Separable Goppa codes have been introduced. The Irreducible and Separable Goppa codes used are with flexible parameters and dynamic error vectors. A Comparison between Separable and Irreducible Goppa code in McEliece Cryptosystem has been done. For encryption stage, to get better result for comparison, two types of testing have been chosen; in the first one the random message is constant while the parameters of Goppa code have been changed. But for the second test, the parameters of Goppa code are constant (m=8 and t=10) while the random message have been changed. The results show that the time needed to calculate parity check matrix in separable are higher than the one for irreducible McEliece cryptosystem, which is considered expected results due to calculate extra parity check matrix in decryption process for g2(z) in separable type, and the time needed to execute error locator in decryption stage in separable type is better than the time needed to calculate it in irreducible type. The proposed implementation has been done by Visual studio C#.

Keywords : McEliece cryptosystem, Goppa code, separable, irreducible
Conference Title : ICCNS 2015 : International Conference on Cryptography and Network Security
Conference Location : Istanbul, Türkiye
Conference Dates : October 26-27, 2015

Open Science Index, Computer and Systems Engineering Vol:9, No:10, 2015 publications.waset.org/abstracts/37017.pdf