Skew Cyclic Codes and Cryptography

BENNENNI Nabil

Faculty of Mathematics USTHB, Algiers, Algeria

USTHB University, Algeria

Abstract

In this article we give a new McEliece cryptosystem based on skew triangular matrix using the automorphism and the skew LDPC codes generated by parity check matrix H, such that to encrypt a message M of length n, we divide it into two blocks message m and $\tilde{m}$ of length α and β respectively.

Keywords

Skew cyclic codes, skew LDPC codes, McEliece cryptosystem based on skew triangular matrix.

.