

MDS matrices are widely used in coding theory and cryptography (e.g. in diffusion layers of block ciphers or hash functions), but the construction of MDS matrices is not at all trivial, especially when we require some other suitable properties (involution, efficiency of implementation). That is why we will deal with the construction of MDS matrices (with other properties) in this thesis. We will show a construction of MDS matrices based on Cauchy matrices and on Vandermonde matrices. Then we will present an algorithm for testing whether a given matrix is MDS. And finally, we will show a construction of MDS matrices based on Companion matrices, which is very convenient for lightweight cryptography.