Лінійні перетворення над скінченними полями характеристики 2, що використовуються в блокових шифрах, на даний час достатньо вивчені, глибоко досліджено їх вплив на стійкість шифру до різного роду атак, чого не можна сказати про перетворення над кільцем лишків за модулем 2^n. Однак використання перетворень над вказаним кільцем дало б змогу підсилювати криптографічну стійкість шифрів як з теоретичної, так і з практичної точки зору.

У даній роботі досліджувались криптографічні властивості перетворень, лінійних відносно додавання за модулем 2^n, зокрема, індекс розгалуження таких перетворень. Були вивчені конструкції та властивості лінійних перетворень, що використовуються в сучасних блокових шифрах, а саме MDS-матриці над скінченними полями характеристики 2. Було визначено, що для кілець $\mathbb{Z}_p$ за простим модулем існують аналогічні конструкції матриць та було знайдено їх кількість. Однак над кільцем $\mathbb{Z}_{2^n}$ не існує матриць з максимальним індексом розгалуження. Для таких матриць була знайдена верхня межа для індексу розгалуження: так, для матриці розміру $m \times m$ індекс розгалуження не більший, ніж $\frac{2m+4}{3}$. Найбільше можливе значення, а саме m, можуть приймати лише матриці розмірності 2, 3 та 4; прикладами таких матриць є сімейство матриць Мідорі.

MDS-МАТРИЦЯ, MAXIMUM DISTANCE SEPARABLE, РЮЗСІЮЮЧИЙ ШАР, ІНДЕКС РОЗГАЛУЖЕННЯ, ЦИРКУЛЯНТНА МАТРИЦЯ, МАТРИЦЯ КОШІ, МАТРИЦЯ ВАНДЕРМОНДА, ДОДАВАННЯ ЗА МОДУЛЕМ, КІЛЬЦЕ ЛИШКІВ ЗА МОДУЛЕМ 2^N