

Спосіб криптографічного перетворення інформації полягає в тому, що інформаційну послідовність подають у вигляді бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow) - за допомогою відповідних пристроїв, підстановка (substitution) - за допомогою блоків підстановок (S-блоків); перемішування (permutation) за допомогою блоків перемішування кубиків (P-блоків); функціональні операції ковзного кодування (SlidCode) за допомогою змішаних кодів Грея. Бітні блоки інформаційної послідовності подають у вигляді тривимірних матриць (кубиків), як S-блок формують змінну тривимірну матрицю підстановок, що будується отриманням мультиплікативно зворотного елемента x^{-1} над розширеним кінцевим полем Галуа $GF(2^8)$ та шляхом виконання афінного перетворення $y = M \cdot x^{-1} + \beta$ над примітивним двійковим полем Галуа $GF(2)$. Як матрицю M афінного перетворення використовують змінні обернені симетричні матриці, які вибирають відповідно до значення циклового ключа, функціональні операції ковзного кодування та підстановки не фіксовані, а залежать від стану ключа. Ітеративна обробка примітивними криптографічними перетвореннями відбувається у такій послідовності: функціональні операції ковзного кодування (SlidCode), перемішування (permutation), підстановка (substitution), функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow).