Кафедра 42
Криптология и дискретная математика
Тел. 324-7334; факс. 323-9137; e-mail: kaf42@mail.ru.
Факультет "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

Исследование преобразований двоичных векторных пространств, максимально удаленных от множества треугольных преобразований

Исполнитель: Котов Андрей Владимирович
МИФИ, «Информационная безопасность», 4 курс

Цель работы

Выработка рекомендаций по выбору криптографических преобразований, стойких к атакам определенного класса, например, к поиску ключа по известному открытому тексту и шифртексту.

Актуальность проблемы

- Существуют вероятностные методы, позволяющие найти корни системы уравнений, решив её приближение, например, линейное или треугольное.
- Чем больше расстояние по Хэммингу между таблицами исходного преобразования и его приближения, тем сложнее найти решение исходной системы.

Аналогия с бент-преобразованиями

- Бент-преобразования — это преобразования, максимально удаленные от множества линейных преобразований.
- Преобразования, исследуемые в данной работе, — это преобразования, максимально удаленные от множества треугольных преобразований.

Мера близости

- Под расстоянием от преобразования $\psi: V_n \rightarrow V_n$ до некоторого множества Φ преобразований пространства V_n будем понимать расстояние по Хеммингу от ψ до «ближайшего» преобразования множества Φ.
- Обозначение: $d(\psi, \Phi)$.

Теорема

Пусть $\Phi_{\Delta,обр}$ — множество всех обратимых треугольных преобразований пространства V_n.

Тогда

1. Для любого $\psi: V_n \to V_n$

$$d(\psi, \Phi_{\Delta,обр}) \le n2^{n-1}; \qquad (*)$$

2. Верхняя граница (*) достижима при любом натуральном n;

3. Число преобразований ψ, для которых оценка (*) достижима, не меньше $2^{n \cdot 2\wedge(n-1)}$.

Способ построения

- Любое преобразование, такое что его *i*-я координатная функция не зависит существенно от *i*-й переменной, i=1,2,…n, является максимально удаленным от множества треугольных преобразований.
- Преобразование, построенное таким образом, равноудалено от всех треугольных преобразований.

Заключение

- Получена точная верхняя граница для расстояния от произвольного преобразования до множества обратимых треугольных преобразований
- Приведен метод построения преобразований, максимально удаленных от треугольных, т.е. преобразований, обладающих высокой стойкостью к определенного вида атакам
- Произведена оценка снизу числа таких преобразований, которая показывает, что широкий класс преобразований множества V_n не имеет близких треугольных подстановочных преобразований.