**Лекция 15.**  Корреляционный криптоанализ. Базовые и другие корреляционные атаки.

#### **Корреляционные атаки** являются наиболее распространёнными атаками для взлома поточных шифров.

Известно, что работа по вскрытию криптосистемы может быть значительно сокращена, если нелинейная функция пропускает на выход информацию о внутренних компонентах генератора. Поэтому для восстановления начального заполнения регистров корреляционные атаки исследуют корреляцию выходной последовательности шифросистемы с выходной последовательностью регистров.

Существуют следующие подклассы корреляционных атак:

* Базовые корреляционные атаки
* Атаки, основанные на низко-весовых проверках четности
* Атаки, основанные на использовании сверточных кодов
* Атаки, использующие технику турбо кодов
* Атаки, основанные на восстановлении линейных полиномов
* Быстрые корреляционные атаки.

**Базовые корреляционные атаки**

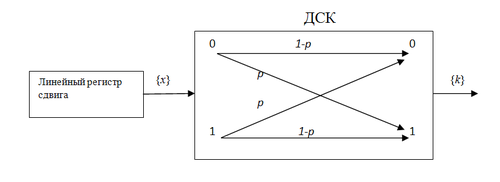


Схема базовой корреляционной атаки

Рассмотрим на примере базовой корреляционной атаки Зигенталера, которая основана на понятии расстояния Хэмминга между двумя двоичными последовательностями одинаковой длины. Применима к комбинирующим генераторам.

Для выявления влияния j-го линейного регистра сдвига. Алгоритм атаки состоит из двух этапов:

1. вычисления корреляционной вероятности ~p_j = P}})исходя из комбинирующей функции ~fи второго этапа.
2. перебор начальных заполнений регистра. На этом этапе определяется наличие корреляции данного фрагмента гаммы ~g с соответствующим фрагментом из ~x_d^{}, путём вычисления функции кросс-корреляции ~C_{{x^{j},{g}}}=\frac{1}{n}*\sum_{i=1}^n^{g_i}*^{x_{i+d}^{}} 

и сравнения этого значения с некоторым числом ~T.

В случае успеха при сравнении, фаза называется верной и происходит переход к следующему регистру ~j+1. Иначе, фаза называется неверной и переходят к ~d=d+1, d=1,2,\dots,2^{L_j}. Выходными значениями этого алгоритма являются состояния ~{x_0^j}, вносящие информацию в гамму.

Теперь немного о подборе порогового значения ~Tи необходимого для успешного криптоанализа количество бит гаммы ~n: Задаём нужные нам вероятности «ложной тревоги» ~P_f=P \ge T|WrongPhase) и пропуска истинного начального заполнения

~P_m=P < T|RightPhase).

Например, выбрали ~P_m=0.01, P_f=2^{-L}, где ~L- длина регистра. А затем из этих условий находим ~Tи ~n.

Атаки, основанные на низко-весовых проверках четности

Примером этого покласса атак может служить быстрая корреляционная атака Майера и Штаффельбаха. Применима она как к фильтр-генераторам, так и комбинирующим генераторам и является базовой для всех остальных быстрых корреляционных атак данного типа. Идея атаки основывается на использовании уравнений проверки четности для полинома обратной связи линейного регистра.

Быстрые корреляционные атаки

Под быстрыми корреляционными атаками подразумеваются атаки, вычислительная сложность которых значительно меньше вычислительной сложности силовых атак.

Этот вид атак сводит проблему декодирования в двоичном симметричном канале к проблеме криптоанализа и моделируется как декодирование случайного ~линейного кода. Аналогично базовым корреляционным атакам, этот подкласс использует понятие расстояния Хэмминга.