НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

АНАЛИЗ МЕТОДОВ КРИПТОАНАЛИЗА ПОТОЧНЫХ ШИФРОВ

Еркаева Наргуль

Преподаватель, Кафедра информатика и информационные технологии Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Мередова Айгуль

студент, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Мередов Даянч

студент, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Магтымова Чынар

студент, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Алгулыев Ашыр

студент, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Пото́чный шифр – это симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста.

Поскольку при разработке любых криптографических схем их стойкость определяется прежде всего стойкостью к известным на текущий момент криптографическим атакам, направленных на выявление в рассматриваемой схеме слабостей различного рода, представляется целесообразным рассмотрение наиболее распространенных и упоминаемых методов (алгоритмов) криптоанализа для выработки рекомендаций относительно конструирования криптографически стойких схем криптопреобразований.

При рассмотрении методов криптоанализа схем поточного шифрования все методы можно условно разделить на три класса: аналитические атаки, статистические и силовые. К аналитическим атакам относят атаки, в которых алгоритм построения атаки основан на аналитических принципах вскрытия криптосхемы. К статистическим атакам относятся атаки, основанные на оценке статистических свойств гаммы шифрующей. К силовым атакам относятся атаки, основанные на принципе полного перебора всех возможных комбинаций ключа.

При проведении криптоанализа схем подразумевается, что атака произошла успешно, если ее вычислительная сложность меньше, чем вычислительная сложность полного перебора всех ключевых комбинаций данного шифра.

Целью данной статьи является рассмотрение аналитических атак, выработка рекомендаций относительно конструирования криптографически стойких схем поточного шифрования.

Аналитические атаки

Все аналитические атаки происходят при допущении, что криптоаналитику известно описание генератора (образующие полиномы, вид нелинейного преобразования), он обладает открытым и соответствующим ему закрытым текстом. Задачей криптоаналитика является определение применяемого ключа (начального заполнения). На рисунке представлены наиболее известные криптоаналитические атаки, применяемые к синхронным поточным шифрам.

Рисунок 1.

1.Корреляционные атаки

Наиболее распространенными и упоминаемыми атаками являются корреляционные атаки в силу специфики построения поточных шифров. Корреляционные атаки используют корреляцию выходной последовательности схемы шифрования с выходной последовательностью регистров для восстановления начального заполнения последних.

Среди атак данного класса можно выделить следующие атаки:

1. Базовые корреляционные атаки.

· Базовая корреляционная атака Зигенталера;

· Корреляционная атака Зигенталера.

2. Атаки, базирующиеся на низковесовых проверках четности.

· Быстрая корреляционная атака Майера-Штаффельбаха;

· Быстрая корреляционная атака Форре;

· Быстрый итеративный алгоритм Михалевича-Голича;

· Быстрая корреляционная атака Чепыжова-Смитса.

3. Атаки, базирующиеся на использовании конволюционных кодов.

4. Атаки, использующие технику турбо кодов.

5. Атаки, базирующиеся на восстановлении линейных полиномов.

6. Быстрая корреляционная атака Чепыжова, Йоханссона, Смитса.

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

2. Компромисс время-память

Целью данных атак является восстановление начального состояния сдвигового регистра по фрагменту шифрующей последовательности при условии, что криптоаналитику известна схема устройства и некоторый фрагмент гаммы-шифрующей. Сложность атаки зависит от длины перехваченной гаммы-шифрующей и размера внутреннего состояния шифра. Данный вид атаки применим, если пространство состояний достаточно мало.

В общем случае атака состоит из двух этапов:

· подготовительный этап, в котором строится большой словарь, включающий все возможные пары «состояние-выход» (одинаковой размерности n);

· основной этап, в котором делается предположение, что шифр находится в определенном фиксированном состоянии, т.е. предположение об определенном заполнении всех ячеек памяти. На основе этих входных данных генерируется выход. Далее просматривается перехваченная выходная последовательность с целью нахождения соответствия со сгенерированным выходом. Если соответствие произошло, то фиксированное состояние с большой вероятностью считается начальным заполнением регистра, в противном случае алгоритм продолжает работать.

3. Предполагать и определять

Основная идея атаки состоит в допущении, что криптоаналитику известны гамма шифрующая, количество сдвигов регистра между выходами схемы, а также полином обратной связи степени r, фильтр-функция f и последовательность точек съема γi, i = 1, …, n.

Восстановление начального заполнения регистра происходит путем восстановления некоторых фрагментов заполнения регистра на основе предположения содержимого некоторых неизвестных фрагментов схемы (содержимое ячеек регистра, элементы нелинейной функции). В общем виде атака имеет следующий вид:

· Предполагается содержимое некоторых ячеек регистра.

·Определяется полное заполнение регистра путем применения линейной

· рекурренты регистра на основе принятых допущений.

· Генерируется выходная последовательность. Если она эквивалентна гамме шифрующей, предположение принимается верным, иначе – переход к шагу 1.

Сложность атаки зависит от конкретной реализации схемы и пропорциональна количеству предположений. Так, количество возможных предположений равно 2x, где x – количество предположений, приведших к успеху.

4. Инверсионные атаки

Предполагается, что известен полином обратной связи, фильтр-функция и последовательность точек съема. Цель данной атаки – восстановление начального состояния сдвигового регистра по фрагменту шифрующей последовательности.

5. Ключевая загрузка, инициализация/реинициализация

Так как единого алгоритма загрузки не существует, каждый раз, в зависимости от используемой структуры схемы, процедуры ключевой загрузки будут различны. Желательной является конструкция, исключающая загрузку ключа посредством линейных операций и нулевое заполнение регистра, каждый бит инициализированного регистра должен быть нелинейной функцией от каждого бита используемого ключа. Использование линейных операций делает возможным применение криптоанализа посредством решения линейных уравнений.

С целью противостояния криптоаналитическим атакам при построении схем поточного шифрования целесообразно руководствоваться следующими требованиями:

· для генерации регистром последовательности максимальной длины и высокой

· линейной сложности данный регистр должен быть основан на примитивном полиноме обратной связи; при использовании нескольких регистров их длины должны быть взаимно простыми;

· для достижения максимальной линейной сложности степень образующего полинома должна быть простым числом;

· минимальная длина регистра должна быть не менее $\ell = 100$ бит, образующий полином иметь приблизительно около $\ell/2$ ненулевых коэффициентов обратной связи;

· содержимое первой и последней ячеек регистра должны являться входными данными к нелинейной функции, множество точек съема для обратных связей ЛРР и множество точек съема для НЛФ должны исключать совместное использование одних и тех же ячеек;

· при построении нелинейных функций данные функции должны удовлетворять

· критериям стойкости: быть сбалансированными, обладать высокой нелинейностью, удовлетворять критерию распространения (обладать корреляционным иммунитетом), иметь высокую алгебраическую степень.

· при длине ключа k бит внутреннее состояние генератора (внутренняя память) должно быть не менее 2k бит;

· каждый бит начального состояния регистра должен являться функцией от нелинейного преобразования всех бит ключа.