Дайте оцінку криптографічної стійкості симетричних шифрів А5, що застосовуються в системах сотового зв'язку

A5 — это поточный шифр, используемый для шифрования GSM (Group Special Mobile), — европейского стандарта для цифровых сотовых мобильных телефонов. A5 состоит из трех РСЛОС длиной 19, 22 и 23. Выходом является XOR трех РСЛОС (Регистры сдвига с линейной обратной связью). В A5 используется изменяемое управление тактированием. Каждый регистр тактируется в зависимости от своего среднего бита, затем выполняется XOR с обратной пороговой функцией средних битов всех трех регистров. Обычно на каждом этапе тактируется два РСЛОС. Существует тривиальная атака на открытом тексте, основанная на предположении о содержании первых двух РСЛОС и попытке определения третьего РСЛОС по ключевой последовательности. Тем не менее идеи, лежащие в основе A5, позволяют проектировать надежные поточные шифры. Алгоритм эффективен и удовлетворяет всем известным статистическим тестам, единственная его слабость — короткие регистры. Варианты A5 с более длинными сдвиговыми регистрами и более плотными многочленами обратной связи позволяют противостоять силовой атаке.

Все методы криптоанализа поточных шифров обычно подразделяют на 3 класса:

· силовые (атака «грубой силой»)

· статистические

· аналитические методы.

Силовые атаки

Атаки путём полного перебора(перебор всех возможных вариантов). Сложность полного перебора зависит от количества всех возможных решений задачи (размера пространства ключей или пространства открытого текста). Этот вид атаки применим ко всем видам систем поточного шифрования. При разработке систем шифрования разработчики стремятся сделать так, чтобы этот вид атак был наиболее эффективным по сравнению с другими существующими методами взлома.

Статистические атаки

Делятся на два подкласса:

· метод криптоанализа статистических свойств шифрующей гаммы: направлен на изучение выходной последовательности криптосистемы; криптоаналитик пытается установить значение следующего бита последовательности с вероятностью выше вероятности случайного выбора с помощью различных статистических тестов.

· метод криптоанализа сложности последовательности: криптоаналитик пытается найти способ генерировать последовательность, аналогичную гамме, но более просто реализуемым способом.

Оба метода используют принцип линейной сложности.

Аналитические атаки

Этот вид атак рассматривается в предположении, что криптоаналитику известны описание генератора, открытый и соответствующий закрытый тексты. Задача криптоаналитика определить использованный ключ (начальное заполнение регистров).

Виды аналитических атак, применяемые к синхронным поточным шифрам:

· корреляционные

· компромисс "время-память"

· инверсионная

· "предполагай и определяй"

· на ключевую загрузку и реинициализацию

· XSL атака.

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.