АНАЛИЗ ГРАФА ОБРАТНЫХ СОСТОЯНИЙ ШИФРА MICKEY

Казимиров А.В., Олейников Р.В.
(Харьковский национальный университет радиоэлектроники, г. Харьков)

Поточные шифры имеют один из самых высоких показателей производительности среди всех видов криптографических алгоритмов, которые используются для обеспечения конфиденциальности. Этот класс алгоритмов не совершенен и имеет ряд недостатков, среди основных - ограниченный период гаммы, что приводит к необходимости периодического изменения вектора инициализации или ключей шифрования.

В 2008 году закончился европейский конкурс eSTREAM, по итогам которого все представленные поточные шифры разделили на две категории, рекомендованные для программной и аппаратной реализации.

Шифр Mickey относится ко второй категории и является одним из поточных шифров, рекомендованных в Евросоюзе для защиты коммерческих конфиденциальных данных. Преимуществом данного алгоритма является высокая производительность и криптостойкость. Существует два варианта шифра - Mickey-80 v2 и Mickey-128 v2 [1, 2]. Оба основаны на комбинации линейного (R) и нелинейного (S) регистров. Алгоритмы принимают на вход два параметра: вектор инициализации (IV) и сеансовый ключ (K).

Приведенная оценка стойкости алгоритма шифрования основывается на том, что криптоаналитик каким-то образом получил состояние регистров. Задача заключается в определении секретного ключа, основываясь на знании содержимого регистров и IV. Используя алгоритм построения дерева обратных состояний, возможно получить некоторые характеристики графа состояний.

Пусть известно состояние регистров R и S. Тогда предыдущие состояния R' S' вычисляются при помощи обратных функции $CLOCK\_X^{-1}$(R,S) [3]. Получение обратного состояния сводится к перебору всех возможных значений входных параметров и исключения невозможных.

Стоит заметить, что предыдущее состояние не всегда определяется однозначно. Количество веток может варьироваться в зависимости от текущего состояния и режима работы шифра. Существуют следующие режимы:

- загрузки ключа и вектора инициализации (K/IV)
- холостого хода (XX)
- генерации гаммы (ГГ)

В зависимости от режима работы шифра мы можем получить три различных дерева состояний. Любое из этих деревьев можно рассматривать как граф переходов или конечный автомат. С деревом связаны такие понятия, как уровень - множество обратных состояний, из которых возможно получить

начальное состояние после определённого количества тактов, и количество точек ветвлений – множество возможных состояний R' и S', из которых можно получить R и S.

Используя алгоритм построения дерева, можно определить вероятности появления точек ветвления, которые приведены в таблице 1. Приведенные вероятности рассчитаны с точностью, ограниченной 18-ю уровнями дерева.

Таблица 1 – Вероятность появления точек ветвления

ТВ	K/IV		XX		ГГ	
	v80	v128	v80	v128	v80	v128
0	29,82	19,8	28,02	28,25	30,14	27,18
1	0,009	10,31	43,77	45,9	40,52	42,81
2	42,29	40,22	27,35	22,94	28,44	29
3	0,01	10,87	-	2,56	-	-
4	26,98	17,03	0,85	0,35	0,9	1,01
6	0,001	1,77	-	-	-	-
8	0,89	-	-	-	-	-

Математическое ожидание для режима K/IV равно 2, а для холостого хода и генерации гаммы - 1. Таким образом, не важно, на каком этапе было получено состояние регистров, так как его всегда можно определить после инициализации IV и ключа.

При помощи метода построения дерева удаётся, в некоторых случаях, нахождение битов ключа. Это становится возможным благодаря высокой вероятности наличия невозможных состояний. Так как с каждым обратным шагом увеличивается вероятность отсекания поддерева со всеми предыдущими состояниями.

1. Babbage S. "The stream cipher MICKEY 2.0" [Electronic resource] / S. Babbage, M. Dodd. Mode of access: WWW.URL: www.ecrypt.eu.org/stream/p3ciphers/mickey/mickey_p3.pdf – Last access: 2011. – Title from the screen.
2. Babbage S. "The stream cipher MICKEY-128 2.0" [Electronic resource] / S. Babbage, M. Dodd. Mode of access : WWW.URL: http://www.ecrypt.eu.org/ stream/p3ciphers/mickey/mickey128_p3.pdf – Last access: 2011. – Title from the screen.
3. Р. Олейников, А. Казимиров, "Оценка количества допустимых внутренних состояний в поточном алгоритме Mickey". "Прикладная радиоэлектроника" том 10 №2, г. Харьков, 2011.