О СТОЙКОСТИ УМЕНЬШЕННЫХ МОДЕЛЕЙ БЛОЧНЫХ ШИФРОВ К ЛИНЕЙНОМУ КРИПТОАНАЛИЗУ

Долгов В.И., Руженцев В.И.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина,14, каф. безопасности информационных технологий,
тел. (057) 702-14-25, e-mail: vityazik@rambler.ru

The reduced scale models of modern block ciphers are proposed. The security of these models to linear cryptanalysis are checked with using of various testing methods. The conclusions about using the various methods of testing the security from linear cryptanalysis of modern block ciphers are made.

Анализ криптографической стойкости современных блочных симметричных шифров (БСШ) является актуальной на сегодняшний день задачей. Для изучения стойкости современных БСШ к линейному криптоанализу обычно используется проверка практического критерия, которая заключается в определении верхней границы вероятности линейных характеристик (ЛХ). Однако этот показатель не может гарантировать стойкость БСШ к линейному криптоанализу. Для больших гарантий стойкости следует проверять теоретический или точный критерий, то есть оценивать вероятности линейных корпусов (linear hull) (ЛК). Но точный критерий можно проверить только для шифров с небольшим размером блока. Целью настоящего доклада является изложение результатов оценки вероятностей ЛК для уменьшенных моделей современных БСШ (размер ключа и размер блока не превышают 16 битов).

В ходе первого этапа исследований были разработаны масштабированные (уменьшенные) модели нескольких БСШ (размер блока и размер ключа 16 битов). У всех масштабированных (уменьшенных) моделей используются подстановки 4 в 4 бита, операция умножения на специальную матрицу размером 2×2 над $GF(2^4)$. В полной версии доклада приводится более полное описание этих уменьшенных моделей.

Для получения значения вероятности ЛК необходимо произвести анализ вероятности ЛК для всех значений ключа, однако практическое решение такой задачи требует достаточно высоких вычислительных затрат. В ходе эксперимента вероятности ЛК оценивались только для одного ключа (все биты равны 0) и для ограниченного набора входных масок (от 1_{16} до 8_{16}). В полной версии доклада обсуждаются возможные погрешности при таком анализе вероятностей ЛК.

Далее был разработан и реализован алгоритм поиска максимальных вероятностей ЛК для масштабированных моделей различных БСШ с различным числом циклов.

Вероятности ЛК были сопоставлены с ожидаемыми значениями вероятностей ЛХ для различных БСШ. В табл.1 представлены данные для уменьшенного варианта шифра Rijndael.

Таблица 1 - Вероятности ЛХ и вероятности ЛК для уменьшенного Rijndael

Число циклов	$\log_2$(максимальная вероятность ЛХ)	$\log_2$(максимальная вероятность ЛК)
2	–3	–2
4	–9	–5,5
6	–12	–5,7
8	–18	–5,7
10	–21	–5,7

Сравнение показало, что вероятности ЛК значительно превосходят вероятности ЛХ. Из табл. 1 также видно, что в то время как вероятность ЛХ с добавлением каждого цикла

снижается, вероятность ЛК при достижении определенного количества циклов перестает уменьшаться.

Далее были определены максимальные вероятности ЛК для масштабированных моделей различных БСШ с различным числом циклов. Полученные данные представлены в табл. 2.

Таблица 2 – Log_2(Максимальные вероятности ЛК)

Шифр	Количество циклов в шифре		
	2	4	8
Rijndael (p_{ls}=4)	-2	-5,5	-5,7
Rijndael (p_{ls}=6)	-2,1	-5,6	-5,7
Калина (p_{ls}=4)	-2,7	-5,7	-5,7
Калина (p_{ls}=6)	-2,9	-5,7	-5,7
Лабиринт (p_{ls}=4)	-1,4	-4,1	-5,7
Лабиринт (p_{ls}=6)	-1,4	-4	-5,7
ADE (p_{ls}=4)	-2	-3,7	-5,7
ADE (p_{ls}=6)	-2,2	-3,4	-5,7
Мухомор (p_{ls}=4)	-1,1	-2,3	-5,7
Мухомор (p_{ls}=6)	-1,2	-2,2	-5,7

Следующим этапом исследований стал анализ влияния параметров различных компонентов БСШ на вероятность ЛК. Рассматривалось влияние на вероятность ЛК максимального значения в таблице линейной аппроксимации для отдельного S-блока для ненулевых входной и выходной маски p_{ls} (см. табл. 2).

Основные выводы:

- для уменьшенных моделей всех БСШ с несколькими циклами существует значительное расхождение между вероятностью ЛХ и вероятностью ЛК;
- для всех БСШ вероятность ЛК значительно превосходит пороговое значение, при котором шифр считается стойким к линейному криптоанализу;
- для всех БСШ при достижении некоторого количества циклов вероятность ЛК перестает уменьшаться;
- максимальная вероятность линейной аппроксимации отдельного S-блока не оказывает существенного влияния на вероятность ЛК.