ПРИМЕНЕНИЕ СЕТЕЙ ПЕТРИ В ЗАДАЧАХ ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Роздымаха Е.А., Фёдоров А.В.
Научный руководитель: канд. техн. наук, доц. Омельченко А.В.
Харьковский национальный университет радиоэлектроники,
Кафедра сети связи
пр. Ленина, 14, г. Харьков, 61166, Украина
Тел.: +38 057 7021 429; e-mail: Rozdy@mail.ru

Abstract — It is offered a mathematical description for S- and P-boxes that are used in ciphers. The model is based on Petri nets. Perspectives of using such model in problems of linear cryptanalysis have been analyzed. Special attention is paid to the high speed ciphers with controlled permutations.

1. Введение

В криптографии различают два способа построения блочных алгоритмов шифрования: на основе схемы Фейстеля и в виде сети *SPN* [1]. При этом и в том и другом случае для решения задач рассеивания и перемешивания входных битов используются комбинации блоков подстановок (*S*-блоки) и перестановок (*P*-блоки). Стойкость шифра к различного вида криптографическим атакам определяется в основном конструктивными особенностями указанных блоков. В свою очередь, подобные шифры могут рассматриваться в качестве дискретно-событийных динамических систем, поведение которых удобно описывать с помощью сетей Петри (СП) [2].

Целью данной работы является анализ перспектив применения сетей Петри в задачах линейного криптоанализа.

2. Основная часть

В базовом методе линейного криптоанализа исследуются линейные соотношения между подмножествами значений заданных разрядов вектора ключа $V \in GF(2)^m$, входного $X \in GF(2)^n$ и выходного $Y \in GF(2)^n$ векторов на предмет наличия статистически устойчивых линейных зависимостей вида [3]

$$a \cdot X \oplus b \cdot Y \oplus c \cdot V = \varepsilon, Y = F(V, X), \qquad (1)$$

где $\varepsilon \in GF(2)$ — константа, $a, b \in GF(2)^n$, $c \in GF(2)^m$ — фиксированные вектора, именуемые масками, $F(V, X)$ — шифрующее преобразование.

Поскольку уравнение (1) справедливо не для всех значений X и V, то говорят о вероятностном характере линейной зависимости. Если при этом выполнено условие независимого случайного и равновероятного выбора значений X и V и вероятность

$$P = \Pr_{X,V}\{a \cdot X \oplus b \cdot Y \oplus c \cdot V = \varepsilon\} \neq \frac{1}{2},$$

тогда говорят о наличии статистически устойчивой линейной зависимости, при этом совокупность $\{a, b, c, p\}$ называется линейной характеристикой шифрующего преобразования. Для проведения линейного криптоанализа составляется таблица линейных характеристик, по которым вычисляются биты ключа [3].

Проиллюстрируем особенности применения СП в задачах криптоанализа на примере скоростных шифров, построенных на базе управляемых перестановок. В общем случае такие шифры представимы в виде многослойной переключаемой сети (ПС) [3].

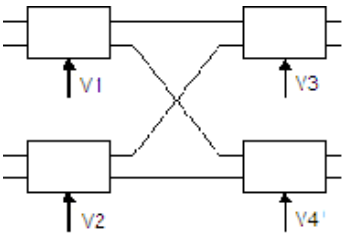

Рис 1 - фрагмент ПС 4x4

На рис. 1 показан фрагмент ПС, включающий в себя четыре блока управляемых по ключу элементарных переключателей. В работе [4] разработана математическая модель в виде СП, описывающая поведение данной ПС. Пользуясь этой моделью мы можем записать систему линейных уравнений, связывающих входной, выходной и управляющий вектор

$$\begin{cases} y_1 = v_3\,(v_1\,x_1 + (1 - v_1)\,x_2) + (1 - v_3)\,(v_2\,x_3 + (1 - v_2)\,x_4); \\ y_2 = (1 - v_3)\,(v_1\,x_1 + (1 - v_1)\,x_2) + v_3\,(v_2\,x_3 + (1 - v_2)\,x_4); \\ y_3 = v_2\,((1 - v_1)\,x_1 + v_1\,x_2) + (1 - v_4)\,((1 - v_2)\,x_3 + v_2\,x_4); \\ y_4 = (1 - v_4)\,((1 - v_1)\,x_1 + v_1\,x_2) + v_4\,((1 - v_2)\,x_3 + v_2\,x_4). \end{cases}$$

Указанную систему уравнений удобно использовать для формироавния таблиц линейных характеристик. Фрагмент такой таблицы для блока 4x4 приведён в табл. 1

Таблица 1

a	*b*	*c*	2*p*	*a*	*b*	*c*	2*p*
0	0	0	0,500	1	2	0	0,125
15	15	0	0,500	1	1	0	0,125

3. Заключение

Поскольку блочные шифры являются динамическими системами, то для изучения их свойств удобно использовать аппарат СП. Математическая модель *S* и *P* блоков шифров в виде СП даёт возможность составить систему уравнений, связывающих входные, выходные воздействия и вектор ключа, что значительно облегчает процесс построения таблицы линейных характеристик, необходимой для проведения линейного криптоанализа.

Эффективность предложенного подхода продемонстрирована на примере криптоанализа скоростных шифров.

4. Список литературы

[1] Бабенко Л.К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. — М.: Гелиос АРВ, 2006. — 376 с.
[2] B. Hrúz Modeling and Control of Discrete-event Dynamic Systems with Petri Nets and Other Tool / B. Hrúz, M.C. Zhou. — London: Springer-Verlag, 2007. — 351 p.
[3] Криптография: скоростные шифры. / А.А. Молдовян, Н.А. Молдавян, Н.Д. Гуц, Б.В. Изотов. — СПб: БХВ Петербург, 2002. — 496 с.
[4] Роздымаха Е.А. Математическая модель скоростных шифров / Е.А. Роздымаха, А.В. Федоров // Мат. 5-й междунар. молод. науч.-техн. конф. «Современные проблемы радиотехники и телекоммуникаций «РТ-2009». — Севастополь: СевНТУ, 2009. — С. 235.