К ВОПРОСУ ОЦЕНКИ КРИПТОГРАФИЧЕСКИХ СВОЙСТВ ПОДСТАНОВОК СЛУЧАЙНОГО ТИПА

В.И. Долгов, И.В. Лисицкая, Р. В. Сергиенко, А.Е. Обухов
Харьковский национальный университет радиоэлектроники,
61166, Харьков, пр. Ленина, каф. БИТ,
e-mail: gorbenko@kture.kharkov.ua.

The given work is devoted to comparative evaluation of two S-block selection methods for symmetric block ciphers. The first one is based on the evaluation resistance component of Boolean functions, and the second one uses the criteria of substitution selection, based on the theory of probabilities (for number of the inversion, the increases and the cycles). It is shown, that the quality of the substitution selection according the theory of probabilities do not concede the quality of choose according instrument of Boolean functions in practice.

Самые современные традиционные ключевые криптосистемы базируются на идее произведения шифров, которые представляют класс криптосистем, повторяющих сложную операцию, отображающую плайнтекст в шифртекст. Каждое такое повторение (итерация) известно как цикл шифра. Сложная (составная) операция, выполняющаяся в каждом цикле, является обычно комбинацией из набора примитивных операций, таких как сдвиг, линейное преобразование, модульная арифметика (сложение) и подстановку. В частности, комбинация перестановочных и подстановочных операций может привести к криптографически сильному нелинейному преобразованию, если оно применяется достаточное число раз. Подстановочные операции во многих шифрах выступают при этом как основной нелинейный элемент циклового преобразования. Поэтому значительные усилия исследователей направлены на изучение подходов к построению подстановок с высокими криптографическими показателями.

Сегодня наиболее разработанным и наиболее популярным математическим аппаратом оценки криптографических свойств нелинейных элементов замены стал аппарат линейной алгебры и в частности булевых функций. Его развитию и применению посвящено большое число публикаций. Предложено и используется множество критериев и показателей оценки свойств самих булевых (компонентных) функций S-блоков, так и критериев и показателей криптографических свойств S-блоков в целом. В их числе такие как: сбалансированность булевой функции, нелинейность N_f, корреляционный иммунитет, критерий распространения (строгий лавинный критерий) $KP(k)$, алгебраическая степень булевой функции $\deg(f)$, а также соответствующие характеристики S-блоков – критерий битовой независимости (BIC), критерий нелинейности, максимальный порядок строгого лавинного критерия ($MOSAC$), максимальное значение линейной аппроксимационной таблицы-LAT, δ-гладкость (равномерность) XOR-таблицы S-блока и многие другие.

В то же время нами был предложен подход к отбору подстановок [1-3], строящийся на основе оценки показателей их случайности (значений числа циклов, возрастаний и инверсий, дополненных ограничениями на максимально допустимые значения таблиц дифференциальных разностей и линейных аппроксимаций). Уже давно возникло естественное желание найти связь между отмеченными подходами и, в частности, оценить место и полезность критериев

случайности в общем комплексе вопросов, связанных с решением задач построения криптографически стойких подстановочных конструкций.

Целью настоящего доклада является изложение результатов применения и сопоставления для оценки показателей нелинейности S-блоков одновременно обоих подходов, позволяющих установить интересующую нас связь.

В первой части доклада излагаются результаты оценки показателей нелинейности для подстановочных конструкций на примере подстановок размером 4×4 для шифра ГОСТ и ряда других шифров. Оценка выполняется для целого набора показателей компонентных булевых функций для подстановок, удовлетворяющих заданным критериям случайности.

Рассматриваются подстановки, входящие в долговременный ключ ГОСТа, заимствованный из публикации [4], а также подстановки, построенные ЭВМ по нашим правилам. Кроме того, рассматриваются подстановки соответствующего размера встречающиеся в публикациях.

Во второй части доклада приводятся результаты применения рассматриваемых подходов к подстановкам размера 8×8. Здесь определяются показатели случайности подстановок используемых в ряде современных шифров AES-Rijndael, FOX, Лабиринт, Калина, Мухомор и др. Результаты подтверждают, что подстановки, используемые в современных шифрах, удовлетворяют установленным критериям случайности.

В третьей части доклада приводятся результаты статистических экспериментов, посвященных распространению результатов проверки соответствия показателей компонентных булевых функций на представительное множество подстановок случайного типа.

Результаты свидетельствуют, что случайные подстановки, прошедшие предложенные критерии отбора, обладают высокими криптографическими свойствами и при оценке их показателей нелинейности с помощью аппарата булевой алгебры.

Список ссылок

1. Горбенко И.Д., Лисицкая И.В. Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 28147-89 //. Радиотехника. Всеукр. межвед. науч.-техн. сб. 1997. Вып 103. С. 121–130.

2. Лисицкая И.В. К вопросу построения долговременных ключей для алгоритма ГОСТ 28147-89 // Информационно-управляющие системы на железнодорожном транспорте. 1997. № 3. С. 54–57.

3. Lysytska I.V., Koriak A.S., Golovashich S.A., Oleshko O.I., Oleinik R.V. The selection criteria of random substitution tables for symmetric enciphering algorithms // Abstracts of XXVIth General Assembly. Toronto, Ontario Canada, August 13-21, 1999. - P. 204.

4. Месси Дж. Введение в современную криптологию // ТИИЭР. - 1988. - Т. 76, №5. - С. 24-42.