УДК 681.3.06

И.В. Московченко

Центр подготовки сержантов, Харьков

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ И ВЫЧИСЛИТЕЛЬНЫЙ МЕТОД ПОСТРОЕНИЯ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Математическая модель

Для формализации процесса преобразования данных в диссертационной работе предложена математическая модель, описывающая внутреннюю структуру нелинейного узла замен которая состоит из множества входных векторов A задающих боки открытого текста, множества выходных векторов B задающих блоки закрытого текста, множества отображений каждое из которых параметризируется совокупностью компонентных криптографических булевых функций, системы ограничений по сбалансированности все функции должны быть сбалансированы, если все они сбалансированы, значит S-бокс является сбалансированным, нелинейность всего S-бокса определяется минимальной нелинейностью каждой булевой функции, корреляционный иммунитет выбирается по критерию минимального риска, критерий распространения степени k выбирается также по минимальному значению, автокорреляция функции выбирается максимальной, таким образом, выбираются худшие варианты для каждой булевой функции.

Вычислительный метод

В диссертационной работе предлагается метод построения криптографических булевых функций, основанный на методе градиентного подъема, позволяющий строить высоко нелинейные булевы функции с высокой алгебраической степенью и низким значением автокорреляции. По вычислительным затратам он не превосходит известные ранее методы, а по большинству показателей эффективности превосходит ближайшие аналоги.

При разработке предлагаемого метода в качестве основы взят эвристический метод градиентного подъема В. Миллана, Э. Кларка, Э. Доусона. Данный метод основан на преобразовании выходных последовательностей нелинейных функций.

Суть данной работы состоит в повышении нелинейности произвольной булевой функции путем комплементации некоторой позиции в таблице истинности данной функции. Каждая позиция таблицы истинности соответствует уникальным входным

данным функции. Метод позволяет создать полный список/перечень таких входных данных функции, что комплементация любой соответствующей данному входу выходной позиции в таблице истинности будет увеличивать нелинейность данной функции.

Эффективным путем решения данной задачи, является использование в качестве входных данных не последовательностей, сгенерированных случайным образом, а бент-последовательностей (бент-функций), что позволит качественным образом понизить вычислительную сложность данных методов и добиться высоких показателей стойкости.

Концепция построения предложенного метода базируется на использовании в качестве входных данных бент-последовательностей, обладающих заведомо привлекательными криптографическими свойствами. Целью метода является минимально-возможное понижение нелинейности для приведения ее к сбалансированному виду, что позволяет получить криптографическую функцию с высокими показателями стойкости.

Вывод

В результате исследований решена важная научная задача, состоящая в разработке математических моделей и вычислительных методов построения нелинейных узлов замен с улучшенными свойствами для повышения эффективности симметричных криптографических средств защиты информации.

Список литературы

1. Головашич С.А. Метод построения управляемых S-блоков с предельными показателями нелинейности / С.А. Головашич // Радиотехника: Всеукр. межведомственный научно-техн. сб. – 1999. – № 110. – С. 84-90.

2. Кузнецов А.А. Построение криптографических функций с использованием метода градиентного спуска / А.А. Кузнецов, Ю.А. Избенко, И.В. Московченко // Системи озброєння і військова техніка. – Х.: ХУ ПС, 2006. – Вип. 4 (8). – С. 70-74.

3. Carlet C. Partially – Bent Functions / C. Carlet // Advanced in Cryptology – Crypto'92, New-York: Springer-Verlag, 1993. – P. 280-291.

.