УДК 681.3.06

А.А. Кузнецов[1], С.А. Исаев[2]

[1]*Харьковский национальный экономический университет, Харьков*
[2]*Харьковский национальный университет им. В.Н. Каразина, Харьков*

ИССЛЕДОВАНИЕ ВЕРОЯТНОСТНЫХ МЕТОДОВ ФОРМИРОВАНИЯ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН

Вероятностные методы формирования нелинейных узлов замен (S-блоков) являются одним из перспективных направлений исследований в современной криптографии [1 – 8]. Любой S-блок может быть представлен в виде совокупности булевых функций. В этом представлении оценка стойкости блока замен основа на показателях эффективности булевых функций, которые описывают S-блок.

Пусть B – булева функция, которая описывает i-й бит S-блока, S-блок реализуется через m-кортеж соответствующих функций. Для того, чтобы S-блок был стойким, каждая составляющая его функция и их линейные комбинации должны удовлетворять заданным критериям стойкости: сбалансированности, нелинейности NL, автокорреляции AC, алгебраической степени Deg и строгому лавинному критерию SAC.

Пусть S-блок реализуется через m-кортеж m-битных функций. Пусть есть множество сбалансированных булевых функций, которые удовлетворяют некоторым заданным критериям и пусть есть множество m-битных перестановок таких, что все их линейные комбинации принадлежат данному множеству. Маловероятно, что случайный поиск эффективно найдет отображения. Другим подходом является побитовый метод, состоящий в нахождении перестановки случайным выбором m m-битных функций. Т.е. побитовый метод формирует множество N сбалансированных m-битных функций, а затем выбирает m функций, которые реализуют перестановку и удовлетворяют накладываемым критериям стойкости. Данный класс методов исследован в [4 – 8].

Целью данной работы является проведение экспериментальных исследований и оценка эффек-

тивности вероятностных методов формирования нелинейных узлов замен. В основе проводимых исследований лежит оценка ожидаемого числа отборов (формирований) нелинейных функций, до того, как искомая перестановка будет найдена.

Полученные результаты показывают, что нахождение m-битных перестановок, удовлетворяющих критериям высокой нелинейности и SAC, используя случайные и побитовые методы, для $m > 6$ – вычислительно неразрешимая задача. Побитовый метод, использующий алгоритм ветвей и границ может быть использован для нахождения 6-битной перестановки, которая удовлетворяет SAC и обладает высокой нелинейностью.

Список литературы

1. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag.

2. Handbook of Applied Cryptography [Электронный ресурс] / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 1996. – Режим доступа к ресурсу: http://www.cacr.math.uwaterloo.ca/hac.

3. An analysis of a class of algorithms for S-box construction. Luke O'Connor. 1994.

4. Webster A.F. On the design of S-boxes / A.F. Webster and S.E. Tavares // Advances in Cryptology, CRYPTO 85. – H.C. Williams ed., Lecture Notes in Computer Science. – 1986. – Vol. 218, Springer-Verlag. – P. 523-534.

5. The structured design of cryptographically good S-boxes // Journal of Cryptology. – 1990. – 3 (1). – P. 27-41.

6. Forre R. Methods and instruments for designing S-boxes / R. Forre // Journal of Cryptology. – 1990. – 2 (3). – P. 115-130.

7. Dawson M.H. A unified framework for substitution box design based on information theory / M.H. Dawson // Master's thesis, Queen's University, Kingston. – Ontario, Canada, 1991.

8. Вероятностная модель формирования нелинейных узлов замен для симметричных криптографических средств защиты информации / Л.С. Сорока, А.А. Кузнецов, И.В. Московченко, С.А. Исаев // Системи обробки інформації. – Х.: ХУПС, 2009. – Вип. 3 (77). – С. 101-104