УДК 621.3.06

ВЫБОР УЗЛОВ НЕЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ АНАЛИЗА АЛГЕБРАИЧЕСКИХ СВОЙСТВ ПОДСТАНОВОК

Иван Горбенко, Роман Олейников, Александр Казимиров

Харьковский национальный университет радиоэлектроники, ЗАО "Институт информационных технологий"

Анотація: **розглянуті критерії і запропоновані показники вибору S-блоків для симетричних криптографічних перетворень з точки зору захисту від алгебраїчного криптоаналізу. Наведено доказ максимально досяжного ступеня перевизначеної системи для S-блоків довільного розміру. Представлені результати аналізу алгебраїчних властивостей S-блоків декількох симетричних блокових шифрів.**

Построение или выбор S-блоков с заданными свойствами для применения в симметричных шифрах является достаточно известной проблемой. Один из первых подходов к выбору узлов нелинейной замены предполагал оценку случайности выбранных перестановок. Позднее критерии выбора были расширены для анализа свойств, позволяющих защитить шифр от статистических атак, в том числе от дифференциального и линейного криптоанализа, а также их модификаций. В работах K. Nyberg и C. Ding были обоснованы предельные достижимые границы вероятностей преобразований разностей и линейных аппроксимаций для *S*-блоков. Их результаты были использованы для выбора нелинейных преобразований при построении шифров Rijndael, Camellia и др. что обеспечило этим алгоритмам максимальный уровень запаса стойкости к традиционным статистическим видам криптоанализа.

Тем не менее, в открытой литературе позднее был представлен новый подход, позволяющий построить переопределенную систему уравнений над конечным полем для описания всего криптографического преобразования, названный алгебраическим криптоанализом. Оказалось, что применение S-блоков с предельно достижимыми показателями свойств для защиты от статистических видов криптоанализа позволяет получить низкую степень переопределенной системы, описывающей S-блок. Поскольку только эти элементы определяют нелинейность многих шифров, то алгоритмы AES/Rijndael, «Лабиринт» и др. могут быть описаны разреженной переопределенной системой всего лишь второй степени. Практическая стойкость криптографических систем, использующих эти шифры, обеспечивается только лишь отсутствием универсальных методов, позволяющих находить решения систем нелинейных уравнений 2-й степени над конечными полями.

В связи с этим актуальным становится вопрос построения или отбора S-блоков, обеспечивающих защиту симметричных криптографических примитивов от алгебраических атак. Исходя из увеличения сложности выполнения алгебраического анализа, предлагается критерий, позволяющий из некоторого набора выбирать S-блок, применение которого в шифре позволит обеспечить максимальный уровень стойкости к алгебраической атаке по сравнению с остальными S-блокам. Из двух подстановок защищённой от алгебраического анализа является та, у которой:

а) более высокая степень при описании переопределенной системой уравнений;

б) меньше разреженность (меньше количество нулевых термов в системе).

Эти два показателя не исключают полностью алгебраическую атаку, однако позволяют значительно усложнить её. Увеличение степени системы на единицу влечёт за собой и значительное увеличение количества возможных термов, следовательно, большей производительности и требуемого объёма памяти для решения системы уравнений. Сложность решения конечной системы напрямую зависит от её разреженности, соответственно, снижение разреженности ведет к усложнению криптоанализа.

Рассмотрен подход, позволяющий обеспечить защиту перспективных криптографических симметричных примитивов от алгебраического анализа. Приведено обоснование нахождения минимальной степени переопределённой системы, описывающей табличное преобразование «n битов в m битов». В частности, доказано, что все S-блоки с наиболее распространённым размером современных шифров («8-в-8») могут быть описаны переопределённой системой третьей степени (или ниже). Предложены показатели, по которым возможно сравнивать различные S-блоки для выбора лучшего с точки зрения защиты криптографического преобразования от алгебраической атаки. Приведены результаты анализа свойств S-блоков нескольких симметричных блочных алгоритмов шифрования, в том числе представленных на открытый конкурс криптографических алгоритмов.