Криптоанализ алгоритма после конкурса AES

Как и предполагали эксперты, после принятия алгоритма Rijndael в качестве стандарта AES попытки вскрытия этого алгоритма существенно усилились.

Можно сказать, что криптоанализ алгоритма AES стал развиваться, в основ­ном, в следующих четырех направлениях.

Во-первых, были предприняты попытки усиления «классических» атак или применения других известных атак к данному алгоритму. Например, работа [84] описывает атаку методом бумеранга на 6-раундовую версию алгоритма со 128-битным ключом, для выполнения которой требуется 239 выбранных открытых текстов, 271 шифртекстов с адаптивным выбором и 271 операций шифрования.

Во-вторых, имело место применение различных методов криптоанализа на связанных ключах, в частности:

* в работе [406] предложено несколько вариантов атак на связанных ключах на 7- и 8-раундовый AES-192 с использованием невозможных дифферен­циалов;
* комбинация метода бумеранга и связанных ключей предложена в работе

[70]: 9-раундовый AES-192 атакуется при наличии 279 выбранных откры­тых текстов, каждый из которых шифруется на 256 связанных ключах, выполнением 2125 операций шифрования; для атаки на 10-раундовый AES-256 требуется 2114,9 выбранных открытых текстов (включая зашиф- ровывание на 256 связанных ключах) и 2 ' операций; данная атака ис­

пользует слабость процедуры расширения ключа, состоящую в ее недос­таточной нелинейности;

О эта атака была усилена в работе [202], в которой, в частности, предлагает­ся атака на 10-раундовый алгоритм AES-192; для новой атаки требуется 2125 выбранных открытых текстов (на 256 связанных ключах) и 2146'7 операций.

Несмотря на то, что предложенные атаки на связанных ключах являются весьма непрактичными, настораживает тот факт, что атаке подвержены уже 10 из 12 раундов алгоритма AES-192 (и это после всего 5 лет после принятия стандарта AES!)— возникает опасение, что эксперты (указывающие на не­достаточность раундов в алгоритме Rijndael) были правы и полнораундовый алгоритм AES будет вскрыт существенно раньше, чем предполагали экспер­ты института NIST.

В-третьих, многие исследования были посвящены алгебраической структуре алгоритма Rijndael, например:

О в работе [156] найдены линейные соотношения в таблице замен Rijndael (т. е. в единственном нелинейном элементе алгоритма); однако, как и в дру­гих аналогичных работах, каких-либо практических возможностей ис­пользования этого свойства не предложено;

О как показано в работе [149], зашифровывание с помощью Rijndael можно выразить относительно (особенно по сравнению с другими «серьезными» алгоритмами шифрования) простой формулой; авторы не нашли практи­ческого применения данной формулы, но предположили, что она будет использована в реальных атаках в течение ближайших примерно 20 лет;

* в работе [275] показано, что вскрытие алгоритма AES эквивалентно реше-

g

нию системы квадратичных уравнений в конечном поле GF( 2 ).

Попытки использования алгебраических свойств алгоритма для его вскрытия были названы «алгебраическими атаками» [121]. Стоит отметить, что были и работы с попытками доказательства того факта, что простая структура ал­горитма AES не ухудшает его криптостойкости, например, [361].

В-четвертых, больше всего исследований было посвящено атакам, исполь­зующим информацию, полученную по побочным каналам:

* во многих работах содержатся примеры успешного вскрытия различных реализаций полнораундового алгоритма AES с помощью атак по времени выполнения (например, [49]), потребляемой мощности (например, [248]) и атак на основе сбоев (например, [299]); автор [49] (эта работа описывает успешное вскрытие сервера OpenSLL, использующего для шифрования алгоритм AES), в частности, считает, что эксперты NIST при выборе Rijndael в качестве AES допустили весьма серьезную ошибку, посчитав, что время выбора значения из таблицы замен является константной вели­чиной в конкретной реализации; вывод автора таков: выбор Rijndael, ско­рее всего, был ошибочным;
* не меньше исследований (например. [124, 349]) посвящено безопасным (т. е. защищенным от утечки данных по побочным каналам) программным или аппаратным реализациям AES.

Довольно большой список работ, посвященных side-channel-атакам на AES и методам защиты от них, можно найти, например, на ресурсе [373], посвя­щенном криптоанализу AES.

Заключение

Итак, на май 2007 г., по прошествии всего 6 лет после принятия алгоритма Rijndael в качестве стандарта AES, криптоаналитики весьма серьезно про­двинулись во вскрытии данного алгоритма:

* предложена теоретическая атака уже на 10 раундов (из 12) алгоритма AES-192;
* существует множество примеров вскрытия реализаций алгоритма AES с помощью side-channel-атак.

Не правда ли, все это производит впечатление, что эксперты NIST могли ошибиться в выборе алгоритма — победителя конкурса AES?