СРАВНЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ФУНКЦИЙ РАЗВОРАЧИВАНИЯ КЛЮЧА БЛОЧНЫХ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Казимиров А.В.
Научный руководитель – к.т.н., доц. Олейников Р.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. БИТ, тел. (057) 702-14-25),
E-mail: bit@kture.kharkov.ua; факс (057) 702-14-25

It is given a comparative characteristic of various key schedule functions according to performance and key agility requirements.

В Украине проходит заключительный этап открытого криптографического конкурса, предполагающего выбор алгоритма-прототипа национального стандарта блочного симметричного шифра. Шифры «Калина» (разработчик – ЗАО «Институт информационных технологий»), «Мухомор» (Харьковский национальный университет радиоэлектроники) и «Лабиринт» (ЗАО «Криптомаш»), являются финалистами конкурса. Методы, примененные при разработке этих алгоритмов, используют идеи шифров, представленных в конкурсах AES и NESSIE. В то же время в шифрах реализован ряд новых подходов, в частности, при разработке функции разворачивания ключа (ФРК).

Для получения низкой сложности реализации в большинстве известных шифров выбрана сравнительно простая ФРК, для которой возможно нахождение ключа шифрования по одному или нескольким подключам. Такой подход допускает слабые свойства распространения, которые обуславливают существование значительной корреляции между цикловыми ключами. Иллюстрацией недостатков традиционного подхода к построению ФРК стала теоретическая атака на связанных ключах для AES-192 и AES-256, сложность которой значительно ниже полного перебора ключей.

Приводятся результаты сравнительного анализа быстродействия функций разворачивания ключа алгоритмов ГОСТ-28147, DES, AES/Rijndael, SHACAL-2, Camellia, MISTY1, «Лабиринт» и «Калина». Результаты показали, что скорости работы шифров, представленных на национальный конкурс, и функций разворачивания ключа уступают AES/Rijndael за счёт более высокого уровня криптографической стойкости.

Вместе со скоростью выработки подключей была проверена относительная эффективность ФРК (key agility), которая показывает соотношение времени генерации всех подключей ко времени шифрования одного блока. Единственный алгоритм, который не прошёл по этому критерию ($K_A < 1$), оказался DES (при программной реализации). Для остальных алгоритмов время разворачивания ключа шифрования оказалось меньше времени шифрования одного блока, что позволяет применять такие шифры в приложениях, требующей частой смены ключей (например, протоколе SKIP).