АНАЛИЗ И ИССЛЕДОВАНИЕ СХЕМЫ РАЗВОРАЧИВАНИЯ КЛЮЧЕЙ ШИФРА «КАЛИНА»

Дырявый В.С.
Научный руководитель – к.т.н., доц. Олейников Р.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. Безопасности информационных технологий, тел. (057) 702-14-25).

This work is devoted to research and analysis of key expansion scheme of symmetric block cipher “Kalina” proposed as a candidate to a national standard of Ukraine. Statistic properties of “Kalina” 128 bit version were tested by NIST STS. Collision properties were researched on reduced versions of the cipher. Important facts and assumptions were received.

Блочный симметричный алгоритм «Калина» был создан на основе идей, используемых в алгоритме «Rijndael», который стал национальным стандартом блочного шифрования США и де-факто является самым распространенным и широко используемым в мире в настоящее время. Шифр «Калина» является одним из кандидатов на национальный стандарт блочного симметричного шифрования Украины, поэтому сейчас широко ведутся работы по его исследованию.

Схема разворачивания ключей блочного симметричного шифра является одним из его самых важных компонентов, «слабость» или «сила», которого во многом определяет способность шифра противостоять различного рода атакам и успешно выполнять возложенные на него задачи.

Целью данных исследований было изучение схемы разворачивания ключей блочного симметричного шифра «Калина». Была реализована 128-битная версия спецификации, с целью получения статистической выборки, которая была подвергнута тестам из пакета NIST STS (пакет статистического тестирования). Также была выполнена реализация масштабированных моделей шифра «Калина» с соответствующими размерами блока и ключа шифрования 16\16 бит и 32\32 бит. Схемы разворачивания ключей этих моделей были подвергнуты изучению с точки зрения коллизионных свойств. В ходе вычислительного эксперимента было получено число общих ключей, дающих коллизии, их процентное соотношение эмпирической вероятности коллизии и др. характеристики.

В результате, полученные экспериментальные данные полностью подтвердили теоретические предположения о хороших свойствах схемы разворачивания ключей шифра «Калина». Статистические данные, полученные из 128-разрядной версии шифра, успешно прошли все тесты пакета NIST STS. Следует также отметить свойства масштабированных версий шифра: при увеличении размера блока и ключа вероятность появления ключей, дающих коллизии, снижается экспоненциально.