

КОРРЕЛЯЦИОННЫЕ СВОЙСТВА БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ, ПРЕДСТАВЛЕННЫХ НА ОТКРЫТЫЙ КОНКУРС

Дроботько Е.В., Григорьев А.В.

Научный руководитель – д.т.н., проф. Долгов В.И.

Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина, 14, каф. Безопасности информационных технологий, тел. (057) 702-14-25)

Analytical review of correlated characteristic's estimation procedures of encryption transformation is given in the article. Authors provide some new results about an application of these estimation procedures for scaled versions of symmetric block ciphers, e.g. LABIRINT.

Перед Украиной стоит непростая задача принятия стандарта блочного симметричного шифрования. На текущем этапе отобраны четыре претендента: КАЛИНА, ADE, МУХОМОР, ЛАБИРИНТ и необходимо выполнить всесторонний анализ и проверку основных криптографических показателей представленных решений. Выполнение поставленной задачи для современных шифров требует значительных временных и интеллектуальных затрат. Важное значение в этих условиях представляет использование методик, позволяющих ускорить процесс проверки претендентов и выбора наиболее предпочтительного. Одним из возможных путей реализации этого подхода может стать разработка и анализ уменьшенных версий шифров, подлежащих анализу, – подход интенсивно развиваемый последнее время на кафедре БИТ ХНУРЭ.

В порядке реализации этого подхода в настоящем докладе представляются результаты разработки адаптированной к уменьшенным версиям шифров методики выполнения корреляционного анализа.

В основе этой методики лежит использование трех тестов, позволяющих выявить важные в криптографическом смысле статистические связи между «входом и выходом» шифрующего преобразования. Они позволяют оценить показатели статистической безопасности, такие как: степень полноты отображения (d_c), степень лавинного эффекта (d_a), степень строгого лавинного критерия (d_{sa}).

Приводятся результаты выполненного анализа уменьшенных версий шифров Лабиринт и ADE. На основе этого анализа делается вывод, что предлагаемые конкурсные решения по рассмотренным показателям не уступают соответствующим показателям шифра AES, считающегося сегодня одним из признанных прогрессивных решений по построению современных БШ.