УДК 004.421.5

ИССЛЕДОВАНИЕ ЭКСТРАКТОРОВ, ИСПОЛЬЗУЕМЫХ ПРИ ГЕНЕРАЦИИ КРИПТОГРАФИЧЕСКИ СТОЙКИХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Грозов В.А. (Университет ИТМО)
Научный руководитель – к.т.н., доцент Будько М.Ю.
(Университет ИТМО)

Аннотация
Работа посвящена выбору эффективных экстракторов случайности, необходимых для построения генераторов криптографически стойких случайных последовательностей. Предлагается процедура обоснованного выбора экстракторов на основе оценки качества их выходных последовательностей при помощи тестов NIST 800-90B.

Введение. Технологии криптографической защиты информации обычно базируются на использовании генераторов случайных последовательностей, для построения которых необходимы физические источники энтропии. Устранение отклонений и корреляций, существующих в данных от таких источников, выполняется специальными процедурами – экстракторами случайности. Для извлечения из несовершенного источника случайных последовательностей разработано большое количество различных процедур экстракции. При этом отсутствуют явные критерии выбора экстракторов для конкретных приложений.
Целью работы является обоснованный выбор экстрактора для реализации в качестве компонента генератора случайных последовательностей.

Основная часть. Критерием практической пригодности может служить качество выходных последовательностей экстрактора, оцениваемое с помощью min-энтропии. Это соответствует методике, предложенной в документе NIST 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation, 2018.
На основе анализа научных публикаций и патентных источников были выбраны следующие экстракторы с целью их реализации и сравнения: экстракторы Барака, Импальяццо и Вигдерсона (БИВ), Тревизана (ЭТ) и 2-EXT. БИВ – детерминированный экстрактор с тремя входами, основанный на арифметике в поле Галуа и отличающийся гарантированной стабильностью, низкими затратами и высоким быстродействием. ЭТ – seeded-экстрактор Тревизана с одним входом, основанный на идее более эффективного использования дополнительного источника случайности. 2-EXT – экстрактор, состоящий из двух главных компонентов – блендера и вложенного seeded-экстрактора. Его достоинство заключается в самостоятельном формировании seed с помощью специального алгоритма – блендера.
В качестве модельных источников энтропии использовались встроенные генераторы случайных чисел пакета MATLAB (белый гауссовский шум, равномерное, нормальное и биномиальное распределения). Для оценки качества выходных последовательностей использовались методы расчета min-энтропии при помощи пакета тестов, введенных документом NIST 800-90B. Тестирование показало, что все экстракторы имеют достаточно высокое качество для криптографических приложений. Для корректного сравнения таких характеристик экстракторов, как используемые вычислительные ресурсы и скорость работы было выполнено приведение всех экстракторов к близкому уровню качества за счет изменения числа обработок последовательностей в экстракторах.
Результаты исследования подтверждают эффективность рассмотренных экстракторов. Предложен способ приведения экстракторов к сопоставимому уровню качества для их корректного сравнения за счет варьирования количества повторных обработок последовательностей внутри криптографических алгоритмов seeded экстракторов. Контроль качества результирующих последовательностей осуществлялся при помощи набора тестов

NIST 800-90B. Развитием предложенного подхода является использование физических источников случайности.

Выводы. На основе проведенного анализа выбраны три экстрактора для реализации и использования в задачах защиты данных. Осуществлена процедура экстракции выходных последовательностей из данных, полученных от нескольких модельных источников случайности. Проведено тестирование указанных последовательностей пакетом тестов NIST 800-90B, подтвердившее их высокую степень случайности. Предложенный способ приведения экстракторов к сопоставимому уровню качества позволяет выполнять сравнение характеристик эффективности работы экстракторов, показавшее преимущество качества выходных последовательностей seeded-экстракторов.