УДК 004.421.5

ПРИМЕНЕНИЕ АЛГОРИТМА БЛЕНДЕРА ПРИ ГЕНЕРАЦИИ КРИПТОГРАФИЧЕСКИ СТОЙКИХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

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

Аннотация. В работе обсуждается возможность применять алгоритм блендера в качестве функции генерации криптографически стойких псевдослучайных последовательностей. Возможности алгоритма, способствующие повышению качества выходных последовательностей, рассматриваются с точки зрения различных критериев криптостойкости. Приведены преимущества блендера как алгоритма генерации псевдослучайных последовательностей, применимых в задачах криптозащиты, а также результаты численного эксперимента.

Введение. Методы криптозащиты данных требуют использования надежных криптографических примитивов, в частности – генераторов псевдослучайных последовательностей (ПСП). Традиционно генераторы ПСП строятся на основе стойких алгоритмов шифрования. При этом существует противоречие между высокими требованиями к таким генераторам и необходимостью их применения в условиях ограниченности ресурсов. В связи с этим в последнее время очевидно стремление адаптировать существующие алгоритмы к конкретным условиям применения, а также повысить их защищенность за счет комбинирования различных криптоалгоритмов, их модификации, особой организации раундов и внесения дополнительной случайности в ключ, более рациональной реализации вычислительной схемы алгоритма. Представляется интересным использовать в качестве основного компонента генератора ПСП алгоритм так называемого блендера, известного по теоретическим работам в области экстракции случайности.

Основная часть. Для построения функции генерации ПСП предлагается применить алгоритм блендера, входящего в состав известного экстрактора 2-EXT. Получая на вход 2 последовательности битов длины l, алгоритм блендера формирует семейство из l полноранговых матриц размерами l x l, каждая из которых получается из предыдущей путем циклического сдвига и прибавления элемента базиса, вычисленного на основе примитивного полинома в поле Галуа 2^l. Блендер выполняет над входными последовательностями побитовые операции AND и XOR в соответствии со структурой сформированных матриц. Выходная последовательность блендера вычисляется как набор значений полиномов Жегалкина с числом аргументов, равным $2l$. Степень нелинейности полиномов равна 3. Таким образом, в результате обработки $2l$ входных битов с помощью одной матрицы на выходе получается 1 бит информации.
С точки зрения применимости для генерации криптостойких ПСП к достоинствам алгоритма блендера можно отнести следующие:

- Блендер представляет собой одностороннюю функцию.
- Он позволяет получить выходной блок ПСП любого размера.
- Имеет простой в реализации алгоритм и высокую скорость, а также простую аппаратную реализацию.
- Его выходные биты формируются независимо друг от друга, и возможность появления 0 или 1 на той или иной позиции практически равновероятна.
- Изменение одного входного бита влияет на все выходные биты.

Использование блендера в новом качестве – как функции генерации криптостойких ПСП – требует обоснования такого решения.
В настоящее время нет универсального подхода для оценки криптостойкости. Криптостойкая последовательность должна удовлетворять определенным критериям. Она должна иметь статистические свойства, близкие к свойствам истинно случайной последовательности, высокий уровень энтропии, равномерный характер распределения. Последовательность должна иметь большой период и проходить тест на следующий бит. Важной характеристикой также является линейная сложность последовательностей.
Изучение структуры алгоритма блендера показало, что функции, порождающие его выходные значения, относятся к нелинейным полиномам Жегалкина, которые используются при построении S-блоков многих криптографических алгоритмов. Используемые в блендере полиномы с числом аргументов, равным 2*l*, имеют высокую степень нелинейности. Для количественного подтверждения достаточного уровня перечисленных выше криптографических свойств выходных последовательностей применялись пакеты тестов NIST 800-22 и NIST 800-90B, критерий Пирсона, а также построение профиля линейной сложности.

Выводы. Учитывая принадлежность результирующих функций алгоритма блендера к полиномам Жегалкина высокой степени нелинейности, а также данные численного эксперимента по оценке некоторых характеристик выходных последовательностей, можно сделать вывод о возможности его использования для генерации криптографически стойких ПСП. Этот алгоритм также является привлекательным с точки зрения эффективной реализации и уменьшения временных затрат и потребляемой памяти, что делает возможным его применение в задачах защиты информации для киберфизических систем с ограниченными ресурсами.

Грозов В.А. (автор) Подпись

Будько М.Ю. (научный руководитель) Подпись