УДК 004.421.5

ГЕНЕРАЦИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПОМОЩЬЮ БЛЕНДЕРА В РЕЖИМЕ ПОСТОЯННОЙ СМЕНЫ КЛЮЧЕЙ

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

Введение. Генераторы псевдослучайных последовательностей (ПСП) на основе стойких алгоритмов шифрования являются важным компонентом в методах криптографической защиты данных. Важной проблемой при использовании таких алгоритмов является необходимость применять их в условиях ограниченных ресурсов. В связи с этим существует тенденция повышения криптостойкости за счет комбинирования и модификации различных криптоалгоритмов, внесения дополнительной случайности в ключ, использования новых режимов применения и более рациональной организации вычислительной схемы алгоритмов. Возможной альтернативой криптоалгоритмов в качестве функции генерации ПСП является алгоритм так называемого блендера, известного по работам в области экстракции случайности [1], а также применяемого в составе экстрактора 2-EXT [2].

Основная часть. Для построения функции генерации ПСП предлагается применить алгоритм блендера [3]. Получая на вход две последовательности битов длины l, блендер 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. Таким образом, в результате обработки $2l$ входных битов с помощью одной матрицы на выходе получается один бит информации. Выходная последовательность блендера вычисляется как набор значений полиномов Жегалкина с числом аргументов, равным $2l$ и алгебраической степенью, равной 3. Используемые в блендере полиномы имеют высокую степень нелинейности. Полиномы такого типа используются при построении S-блоков многих криптографических алгоритмов.

С точки зрения применимости для генерации криптостойких ПСП к достоинствам алгоритма блендера можно отнести следующие. Его выходные биты формируются независимо друг от друга, а возможность появления 0 или 1 на той или иной позиции практически равновероятна. Изменение одного входного бита влияет на все выходные биты. Блендер позволяет получить выходной блок ПСП любого размера. Он имеет простой в реализации алгоритм и высокую скорость, а также простую аппаратную реализацию [4].

Требуемый уровень криптостойкости ПСП предлагается обеспечить за счет использования «одноразовых ключей» для генерации отдельных блоков результирующей последовательности.

Традиционно применяемые для генерации ПСП криптоалгоритмы имеют постоянный ключ, а их криптостойкость основана на высокой вычислительно сложности за счет многораундовой структуры. В качестве альтернативы предлагается использовать однораундовый алгоритм блендера в сочетании с модификацией ключей на каждом шаге его работы. В этом случае вычислительная сложность обеспечивается необходимостью определения каждого уникального ключа.

Для осуществления генерации ПСП разработан специальный режим, сочетающий использование блендера и сеть Фейстеля. Генерация очередного блока ПСП выполняется блендером, на вход которого подаются вектор инициализации и ключ, которые впоследствии поочередно модифицируются с помощью циклического сдвига влево и меняются ролями. Таким образом, с помощью сети Фейстеля для каждого блока последовательности

формируется уникальный ключ. Постоянная смена ролей ключа и вектора инициализации после каждой итерации сети Фейстеля повышает степень рассеивания и перемешивания, обеспечиваемые алгоритмом.
Для подтверждения возможности использования блендера в составе функции генерации криптостойких ПСП оценивались их линейная сложность, статистические свойства, уровень min-энтропии, близость характера распределения к равномерному. Численное исследование свойств выходных ПСП выполнялась с помощью пакетов тестов NIST 800-22 и NIST 800-90B (используемых, соответственно, для оценки статистических свойств и min-энтропии), критерия Пирсона (близость распределения к равномерному), а также построения профиля линейной сложности.

Выводы. Разработан режим применения блендера в сочетании с сетью Фейстеля для генерации криптостойких псевдослучайных последовательностей. Генерация ПСП выполняется поблочно, причем подаваемые на вход блендера ключ и вектор инициализации поочередно модифицируются путем циклического сдвига битов и в соответствии с организацией сети Фейстеля меняются местами. Результаты численного эксперимента подтверждают правомерность предложенного способа получения криптостойких ПСП. К преимуществам такого способа генерации можно отнести возможность эффективной реализации, экономии времени и потребляемой памяти, что позволяет использовать его для защиты информации в киберфизических системах с ограниченными ресурсами.

Список использованных источников:

1. Dodis Y., Elbaz A., Oliveira R., Raz R. Improved randomness extraction from two independent sources, in Approximation, Randomization, and Combinatorial Optimization // Algorithms and Techniques. – 2004. – Pp. 334-344. DOI: 10.1007/978-3-540-278214_30.
2. Johnston D. Random number generators – principles and practices. A guide for engineers and programmers. DeG Press, 2018.
3. Grozov V., Guirik A., Budko M. Construction of a cryptographically secure pseudorandom sequence generator based on the blender algorithm // Proc. 13th Int. Congress on Ultra Modern Telecommunications (ICUMT). – 2021. – Pp. 156-161. DOI: 10.1109/ICUMT54235.2021.96316034.
4. Грозов В.А. Исследование криптостойкости алгоритма генерации псевдослучайных последовательностей на основе блендера // Информатизация и связь. – 2022. – №3. – С. 31-39. DOI: 10.34219/2078-8320-2022-13-3-31-39.