УДК 681.3.07

УОЛША ГЕНЕРАТОРЫ ПОТОЧНОГО БЛОЧНО-СБАЛАНСИРОВАННОГО ШИФРОВАНИЯ

Белецкий А.Я., д-р техн. наук, профессор,
Белецкий А.А., мл. научный сотр.,
Национальный авиационный университет
(E-mail: abel@nau.edu.ua)
Кузнецов А.А.,,канд. техн. наук, ст. научный сотр.
Харьковский университет воздушных сил
(E-mail: kuznetsov_alex@rambler.ru)

При шифровании больших объемов данных (таких, например, как речь или «живое видео») в реальном времени применяются *поточные* криптографические системы (шифры, генераторы). Суть поточных шифров заключается в сложении по модулю 2 битов потока ключей с битами сообщений. В современных криптосистемах поток ключей (*поточный ключ*) генерируется из короткого основного (*базового*) ключа с помощью однозначно определенных детерминированных алгоритмов, осуществляющих так называемую процедуру *разворачивания ключа*.

Поточные шифры принято разделять на *синхронные* и *самосинхронизирующиеся* (или *асинхронные*). В синхронных поточных шифрах поточный ключ (*гаммирующая функция* или *гамма*) формируется независимо от входной последовательности, каждый элемент (бит, байт и т.п.) которой таким образом шифруется независимо от других элементов. Если же поточный ключ зависит от исходных данных и результата их шифрования, то шифрование называют самосинхронизирующимся. Большинство реализаций поточного шифрования являются синхронными.

В докладе предлагается ***WKG*** семейство поточных криптографических систем, размер секретного ключа ***K*** которых составляет 256 бит. Аббревиатура ***WKG*** порождается ключевыми словами ***W**alsh **K**eystream **G**enerator* (Уолша генератор гаммы). Отличительная особенность семейства ***WKG*** шифров состоит в том, что за один шаг шифрования в системе формируется 256-разрядный блок гаммы, образующийся в результате

стохастической перестановки и циклических сдвигов (перемешивания) элементов (битов) *сбалансированной* (1,0)-матрицы Уолша 16-го порядка. Блок битов (обязательно четного порядка) считается сбалансированным, если содержит одинаковое число нулей и единиц. Симметрическая матрица Уолша трансформируется в сбалансированную (1,0)-матрицу двумя приемами. Во-первых, заменой элементов –1 на 0. И, во-вторых, приведением элементов верхней строки матрицы (состоящей из одних положительных единиц) к сбалансированной последовательности, в качестве которой выбрана чередующаяся (0,1)-последовательность.

Алгоритмы ***WKG*** строятся из двух этапов: *управляющей фазы*, в ходе которой переопределяется состояние регистров ключевого поля и *вычислительной фазы*, в ходе которой формируется 256-битная гамма функция. Различные способы реализации этих двух фаз приводят к различным вариантам ***WKG*** генераторов, включая синхронные и самосинхронизирующиеся шифры. Перечисленным фазам функционирования ***WKG*** алгоритма отвечают два его базовых криптографических объекта. Первым объектом шифрующей системы является управляющий блок, представляющий собой квадратную *матрицу ключевого поля* 16-го порядка, в которую на этапе инициализации загружается базовый 256-битный секретный ключ ***K***. Вторым объектом также служит квадратная матрица 16-го порядка (***W***-матрица), предназначенная для формирования 256-битных блоков сбалансированных псевдо случайных последовательностей (гамма функций). На этапе инициализации в эту матрицу загружается стартовая сбалансированная матрица Уолша-Пэли. Состояние второго криптографического объекта (регистров ***W***-матрицы) находится в прямой зависимости от состояния первого объекта – матрицы (совокупности 16-разхрядных регистров) ключевого поля. Алгоритм изменения состояния регистров ***W***-матрицы сохраняется неизменным для всех типов семейства ***WKG*** шифров, в то время как алгоритм управления состоянием регистров матрицы ключевого поля меняется каждый раз при переходе к новому типу генератора.

В докладе приводится сравнительный анализ эффективности (по критерию качества статистических свойств псевдослучайных последовательностей) четырех типов Уолша генераторов, включая линейные и нелинейные, синхронные и асинхронные. В числе последних рассматривается поточный самосинхронизирующийся Уолша генератор с нелинейной обратной связью по шифротексту.