ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

А.М.Х. Альбатша

ТРЕХМЕРНАЯ МОДИФИКАЦИЯ ГОСТ 28147-89

(Национальный исследовательский ядерный университет МИФИ)

До недавнего времени национальным стандартом шифрования в России являлся ГОСТ 28147-89 с длиной блока и ключа 64 и 256 бит. При всех достоинствах шифра (простая и понятная архитектура, эффективная реализация на 32-разрядной платформе, огромный запас прочности, оригинальная конструкция генератора псевдослучайных чисел), он считается устаревшим ввиду малой длины блока данных, ограничивающей объем обрабатываемой информации на одном ключе. В связи с этим возникла необходимость создания нового шифра, и в качестве нового криптографического стандарта в 2015 г. был утвержден симметричный блочный алгоритм с кодовым названием «Кузнечик», длина блока и ключа которого составляют 128 и 256 бит соответственно и который позволяет в большинстве режимов шифрования обрабатывать на одном ключе до 228 Тбайт информации.

Известно несколько способов «продления жизни», т.е. модификации блочного шифра ГОСТ 28147-89. Так, А.А. Дмух, Д.М. Дыгин и Г.Б. Маршалко предложили использование двух *S*-блоков с целью увеличения стойкости по отношению к атакам, предложенным Изобе и Динуром, Дункельманом, Шамиром; при этом 2-GOST остается пригодным для реализации на низкоресурсных устройствах [3]. М.А. Иванов, А.В. Стариковский и Л.И. Шустова предложили трехмерную модификацию шифра, увеличив разрядность обрабатываемых блоков данных с 64 до 512 бит, что позволяет использовать 3DGOST для синтеза алгоритмов хеширования [1].

В основе алгоритма 3DGOST лежит представление кодируемого массива в виде куба со стороной 8 (размер 8 x 8 x 8), где каждая ячейка – один бит массива. Итого, размер куба – 64 байта. С основными особенностями блочного криптоалгоритма 3DGOST можно ознакомиться в источнике [1]. В настоящем исследовании предпринята попытка совершенствования алгоритма 3DGOST путем расширения ключа (KeyExpansion) от 512 до 576 бит.

В первую очередь, алгоритм был реализован на языке C#. На первом этапе был получен куб из данных массива, используя битовые операции. Для каждого куба выполнялись следующие операции шифрования вдоль осей *x, y, z*:

1. Были получены слои, используя ось *x*.
2. Слои перемешивались по произвольной таблице.

3. Выполнялась операцию шифрования из старого алгоритма ГОСТ в 6 раундов, для чего использовалась часть ключа, соответствующей оси *x* и заданному слою.
4. Были получены слои, используя ось *y*.
5. Слои перемешивались по произвольной таблице.
6. Выполнялась операция шифрования из старого алгоритма ГОСТ в 6 раундов, для чего использовалась часть ключа, соответствующей оси *y* и заданному слою.
7. Были получены слои, используя ось *z*.
8. Слои перемешивались по произвольной таблице.
9. Выполнялась операция шифрования из старого алгоритма ГОСТ в 6 раундов, для чего использовалась часть ключа, соответствующей оси *z* и заданному слою.

На завершающем этапе куб был записан в массив при использовании битовых операций. Операции обработки слоев выполнялись параллельно, с использованием многопоточного режима.

Далее с целью совершенствования полученного в результате преобразований криптоалгоритма 3DGOST ключ длиной 512 бит был расширен до набора ключей общей длиной в 576 бит (32 бита на ключ, 3 измерения, 6 раундов). Расширение ключа (KeyExpansion) было реализовано следующим образом:

1. Был заполнен массив констант раундов.
2. Исходный ключ был разбит на блоки по 32 бита.
3. Для *i* от 0 до 17 была выполнена последовательная операция XOR с блоками от *i* до *i*+18, а затем с константой раунда (при выходе номера блока за пределы массива, переходили к 0).
4. Полученное значение является 32-битным ключом для раунда *i*.

Данное преобразование существенно увеличивает криптостойкость алгоритма ГОСТ 28147-89, поскольку позволяет расширить ключ от 256 битов, изначально присущих ГОСТу, до 576 бит. Тестирование трехмерной версии ГОСТ 28147-89 было проведено по методике NIST [2] и показало статистическую безопасность алгоритма.

Литература

1. Иванов, М.А. Новая жизнь старого ГОСТа: переход от одномерной версии к 3D [Текст] / М.А. Иванов, А.В. Стариковский, Л.И. Шустова // REDS: Телекоммуникационные устройства и системы, 2017. – Т. 7. – № 4. – С. 488–491.

2. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22. Revision 1.a. April, 2010 [Электронный ресурс]. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf

3. Dmukh, A.A. A lightweight-friendly modification of GOST block cipher [Текст] / A.A. Dmukh, D.M. Dygin, G.B. Marshalko // Математические вопросы криптографии, 2014. – Т. 5. – Вып. 2. – С. 47–55.