


КОД БЕЗОПАСНОСТИ

О ключевом расписании на основе модифицированного аддитивного генератора

Докладчик: Коренева А.М.

Авторы: Фомичёв В.М., Задорожный Д.И., Коренева А.М., Тулебаев А.И.

Актуальность работы

- Ключевое расписание (КР) определяет криптографическую стойкость блочного шифра относительно ряда методов: согласования, дифференциального криптоанализа и др.

- Применение многих методов криптоанализа не эффективно, если КР обеспечит сложную зависимость раундовых ключей от битов основного ключа.

Простое КР	Более сложное КР
DES, IDEA, ГОСТ 28147-89	AES, ГОСТ Р 34.12–2015 («Кузнечик»)

Цель работы

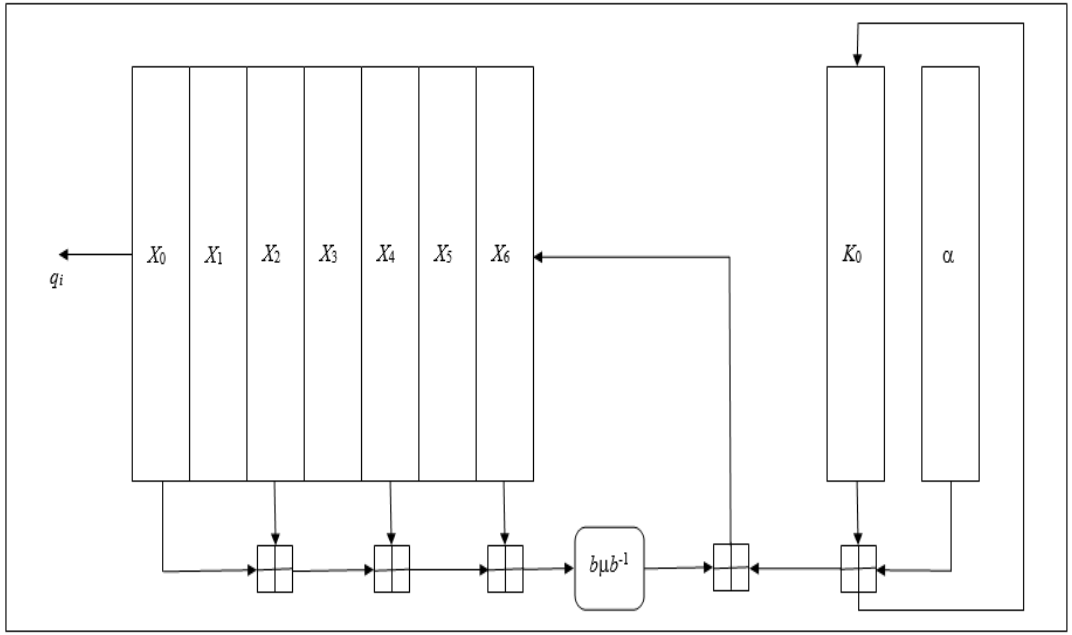
Построение **«гибкого»** алгоритма КР, допускающего различные длины основного ключа ($128+32k$ бит, $k=0,1,2,3,4$) и обладающего свойствами:

- **совершенная зависимость** раундовых ключей, то есть существенная зависимость каждого бита раундовых ключей от всех битов основного ключа;
- успешное прохождение известных **статистических тестов**;
- быстрая **программная реализация** с использованием современных вычислительных средств.

Генератор ключевого расписания (КР)

Генератор $\boldsymbol{G_\mu}$ построен на основе последовательного соединения полноциклового линейного конгруэнтного генератора (**ЛКГ**) с модулем $m=2^r$ и нечётным сдвигом α и аддитивного генератора длины n, модифицированного с помощью преобразования μ (**МАГ-μ**). Конструкция гарантирует длину периода выходной последовательности, кратную m.

Обозначения на схеме:
$X_0,\ldots,X_6,K_0 \in Z_m$;
$\boxplus$ — операция сложения в кольце вычетов Z_m;
b — отображение $Z_m \leftrightarrow V_r$, определяющее двоичное r-разрядное представление числа;
μ — преобразование множества V_r;
b^{-1} — обратное к b отображение;
q_i — элемент выходной последовательности генератора, $q_i=X_i$, $i\geq 0$.



Перемешивающие свойства генератора (1)

При n=7, r=32, D={0,2,4,6} закон рекурсии состояний генератора G_μ имеет вид:

$$X_{i+7} = b^{-1}(\mu(b((\sum_{s\in D} X_{i+s}) \bmod 2^{32}))),\ i\geq 0,$$

Функция переходов h^μ генератора G_μ, имеет вид: $h^\mu(X_i,\ldots,X_{i+6},K_i) = (X_{i+1},\ldots,X_{i+7},K_{i+1})$, $i\geq 0$.

Перемешивающие свойства генератора G_μ близки к наилучшим, если **перемешивающий орграф** $\Gamma(h^\mu)$ преобразования h^μ является локально **примитивным** и в перемешивающем орграфе подстановки μ с множеством вершин {0,1,…,31} вершина 31 достижима из вершины 0 [Fomichev V. M., Koreneva, A.M. Mixing properties of Modified Additive Generators (Journal of Applied and Industrial Mathematics, 2017).

В качестве μ исследованы подстановки на множестве V_{32}:

1. Циклический сдвиг координат векторов на 1 шаг:

$$\mu_1(y_0,\ldots,y_{30},y_{31})=(y_1,\ldots,y_{31},y_0).$$

2. Подстановка вида:

$$\mu_2(y_0,\ldots,y_{30},y_{31})=((y_4,\ldots,y_7)\oplus S(y_0,y_1,y_2,y_3),\ (y_8,\ldots,y_{11})\oplus S(y_0,y_1,y_2,y_3),\ldots,$$
$$y_{28},\ldots,y_{31})\oplus S(y_0,y_1,y_2,y_3),\ S(y_0,y_1,y_2,y_3)),$$

где S – один из s-боксов, определённый в МР 26.2.003-2013 «Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89».

Перемешивающие свойства генератора (2)

Локальный (0,256)-экспонент перемешивающей матрицы M (матрица смежности вершин 256-вершинного орграфа $\Gamma(h^{\mu})$) определим как наименьшее натуральное число $\boldsymbol{\gamma_0}$ такое, что при любом натуральном $t \geq \gamma_0$ у матрицы M^t все столбцы с номерами 0,1,…,31 положительны. Локальный экспонент **оценивает снизу** число тактов работы генератора, после которых каждый знак генерируемого вектора зависит от всех битов начального состояния.

Показателем 0-совершенности назовём наименьшее число $\boldsymbol{\gamma}$ тактов работы генератора, после которых каждая координатная функция 0-го блока $\bar{X}_0$ зависит существенно от всех битов начального состояния $(\bar{X}_0,\ldots,\bar{X}_6,\bar{K}_0)$.

Проведён вычислительный эксперимент по определению значения γ, в ходе которого опробовано порядка 2^{20} пар двоичных векторов длины 256, соседних по каждой из координат. Значения γ_0, γ для генератора G_{μ} приведены в таблице:

	γ_0 / γ
μ_1	9 / 21
μ_2	8 / 12

Совершенная зависимость имеет устойчивый характер: сохраняется как минимум до (γ+500)-го такта работы генератора.

Получение раундовых ключей и оценка программной реализации генератора

Основной ключ длины $128+32k$ бит, $0 \le k \le 4$, есть начальное заполнение $(\bar{X}_0,\ldots,\bar{X}_{2+k},\bar{K}_0)$ генератора. При $k<4$ начальные заполнения некоторых ячеек фиксированы.

Последовательность раундовых ключей образуется как детерминированная нерегулярная выборка из последовательности $\{\bar{X}_i\}$, $i \ge \gamma$, что обеспечивает требуемую совершенную зависимость.

С помощью тестирования программной реализации генератора G_μ на языке *C++* на компьютере с характеристиками Intel(R) Core(TM) i-3550 CPU, 3.30 GHz установлено, что **за 1 такт процессора** при обеих модификациях реализуется около **5 тактов работы генератора** G_μ (вычислено с помощью счётчика RDTSC, флаг оптимизации O2).

В среднем за 25 тактов генератор формирует 100 32-битовых раундовых ключей (3200 ключевых бит) из основного ключа. Для вычислений всех выходов генератора достаточно 72-77 байтов оперативной памяти (в зависимости от модификации).

Статистические свойства выходных последовательностей

Для проверки статистических свойств генератора G_μ при различных начальных заполнениях генератора и значениях параметра α (α=7, α=65535, α=171189289) сформированы файлы по 256 МБ выходных данных ($2{,}147 \cdot 10^9$ бит).

- **NIST STS**

Материал исходного файла разбивался для анализа на 200 подпоследовательностей по 10^7 бит. Параметры тестирования выбирались согласно рекомендациям NIST [**A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications Special (Publication 800-22 Revision 1a, April 2010)**].

- **Wolfram Mathematica**

Исходные файлы анализировались полностью и для тестирования применялись критерии: частот знаков двоичной последовательности, частот «знакоперемен», хи-квадрат согласия с равномерным распределением частот байт.

Все последовательности успешно прошли статистические тесты для критериев с уровнем значимости 0,01, превышение граничных значений статистических критериев не наблюдалось, то есть подтверждены хорошие статистические свойства генератора.

Для всех тестируемых двоичных последовательностей наблюдалось стабильное отклонение вероятности знака от ½ порядка 10^{-6}.

Выводы

Предложен генератор ключевого расписания со свойствами:

- длина периода выходной последовательности кратна 2^{32};
- «гибкость» алгоритма – генерирует 32-битовые раундовые ключи из основного ключа варьируемой длины от 128 до 256;
- совершенная зависимость раундовых ключей от основного ключа;
- быстродействие программной реализации;
- хорошие статистические свойства ключевого материала.

Спасибо за внимание!