УДК 681.324.067

АНАЛИЗ АВТОКОРРЕЛЯЦИОННЫХ ФУНКЦИЙ СЛУЧАЙНЫХ СИГНАЛОВ

А.А. ТОРБА, В.А. БОБУХ, А.А. ТОРБА

В работе рассматриваются результаты экспериментальных исследований аппаратных генераторов случайных последовательностей и их автокорреляционных функций.

Ключевые слова: автокорреляционная функция, аппаратный генератор случайных последовательностей.

ВВЕДЕНИЕ

Теоретически достижимый уровень скрытности известных криптографических систем в значительной степени определяется статистическими свойствами аппаратного генератора случайных последовательностей (АГСП), построенного на основе физического датчика шума. Этот АГСП используется для формирования ключевых данных, случайных параметров, синхромаркеров и др. Важным свойством АГСП является независимость случайных битовых последовательностей, т.е. формирование каждого следующего случайного бита не зависит от значений всех ранее сгенерированных битов.

Наиболее часто в современных криптографических системах используются датчики шума на основе кремниевых диодов с Зенеровским пробоем [1]. В базовой схеме генерации случайных последовательностей (см. рис. 1) [1] аналоговый случайный сигнал физического датчика шума (с частотой случайных импульсов *Fш*) преобразуется в уровни цифровых сигналов при помощи компаратора с небольшим гистерезисом (TS). Счетный триггер (T) выравнивает вероятности цифрового случайного сигнала. Этот сигнал записывается в сдвигающий регистр RG с частотой *Fo*. Частота – *Fo* – определяет скорость формирования цифровой случайной последовательности. После заполнения сдвигающего регистра параллельный код передается в ПЭВМ.

При тестирование статистических параметров случайной последовательности в ПЭВМ наиболее часто для определения независимости формируемых случайных последовательностей используют автокорреляционный тест [2].

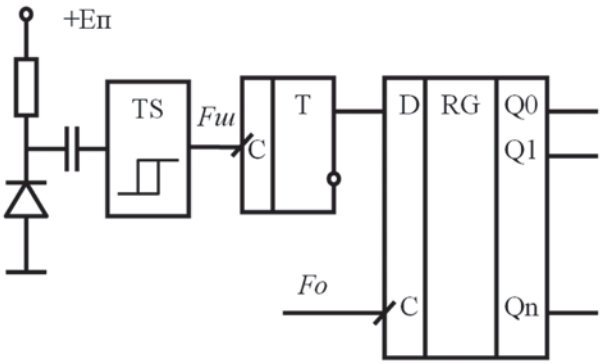


Рис. 1. Базовая схема генерации случайных последовательностей

1. ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СООТНОШЕНИЯ

Для расчета коэффициентов автокорреляционной функции случайной битовой последовательности длиной L_s выбирают начальный участок длиной: $L_a < L_s$. Участок битовой последовательности L_a сдвигают на один бит и сравнивают с исходной битовой последовательностью. Количество битовых сдвигов определяет аргумент – τ – для коэффициентов автокорреляционной функции (на рис. 2 количество сдвигов равно: $\tau = 3$).

Сравнение битовых операндов выполняется логической операцией «ИСКЛЮЧАЮЩЕЕ ИЛИ» (операцией XOR, «суммирование по модулю 2»). При одинаковых битах на входах логического элемента XOR результат сравнения равен логическому нулю, при разных входных битах – результат равен логической единице. Схемы суммирования рассчитывают сумму совпадающих битов – $\Sigma_{\text{совпад}}$ и сумму несовпадающих битов – $\Sigma_{\text{несовп}}$. Коэффициенты автокорреляцион-

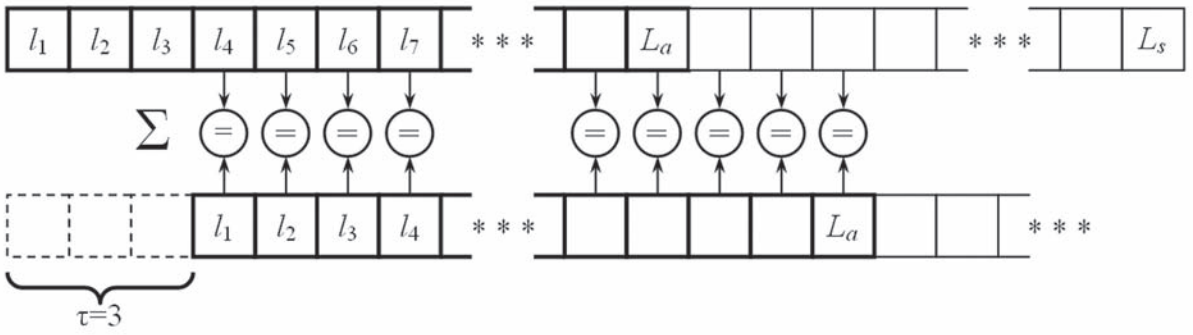


Рис. 2. Алгоритм вычисления автокорреляционной функции

ной функции $K(\tau)$ рассчитываются как разности этих сумм:

$$K(\tau) = \Sigma_{\text{совпад}} - \Sigma_{\text{несовп}}, \quad (1)$$

где: τ – количество битовых сдвигов случайной последовательности.

Обычно подсчитывают только количество единичных битов на выходе элементов XOR (т.е. количество несовпадений), поэтому:

$$K(\tau) = L_a - 2 \cdot \Sigma_{\text{несовп}}. \quad (2)$$

Коэффициент автокорреляционной функции при нулевой задержке ($\tau = 0$) численно равен дисперсии случайного процесса, поэтому (с учетом полного совпадения всех битов) дисперсия равна:

$$K(0) = D = L_a. \quad (3)$$

Нормированные коэффициенты автокорреляционной функции :

$$k(\tau) = K(\tau) / K(0) - \quad (4)$$

всегда меньше единицы.

Нормированные коэффициенты автокорреляционной функции можно рассчитать по условным вероятностям переходов случайных битов в последовательности (рис. 3). Вероятности формирования случайных битов: $P(x0) = P(x1) = 0{,}5$. Вероятности формирования следующего случайного бита: $P(x^+0) = P(x^+1) = 0{,}5$.

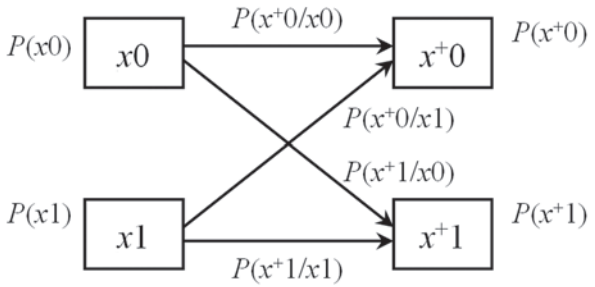


Рис. 3. Вероятности переходов случайных битов

Условные вероятности перехода следующего бита в противоположное состояние: $P(x^+0/x1) = P(x^+1/x0)$.

Условные вероятности сохранения предыдущего состояния бита: $P(x^+0/x0) = P(x^+1/x1)$.

В этих соотношениях учитывается:

$$P(x^+0/x0) + P(x^+1/x0) = 1, \quad (5)$$

потому что после нулевого предыдущего бита ($x0$) будет переход или в нулевое состояние (x^+0), или в единичное состояние (x^+1) с суммарной вероятностью, равной единице.

Аналогично:

$$P(x^+1/x1) + P(x^+0/x1) = 1. \quad (6)$$

При формировании независимых соседних случайных битов условные вероятности равны:

$$P(x^+0/x1) = P(x^+1/x0) = P(x^+0/x0) = P(x^+1/x1) = 0{,}5. \quad (7)$$

При наличии корреляционных связей между соседними случайными битами условные вероятности различны:

$$P(x^+1/x1) - P(x^+0/x1) = P(x^+0/x0) - P(x^+1/x0) = \varepsilon. \quad (8)$$

Величина разности условных вероятностей – ε – меньше единицы по модулю и может принимать положительные или отрицательные значения. Для статистически независимых случайных битов эта разность равна нулю: $\varepsilon = 0$.

С учетом соотношений (1), (3), (4), (5), (6), (8) нормированные коэффициенты автокорреляционной функции равны:

$$k(\tau) = [P(x0) \cdot P(x^+0/x0) + P(x1) \cdot P(x^+1/x1)] - [P(x0) \cdot P(x^+1/x0) + P(x1) \cdot P(x^+0/x1)] = \varepsilon(\tau), \quad (9)$$

где: $P(x0) \cdot P(x^+0/x0) = P(x0, x^+0)$ – вероятность сохранения нуля; $P(x1) \cdot P(x^+1/x1) = P(x1, x^+1)$ – вероятность сохранения единицы; $P(x0) \cdot P(x^+1/x0) = P(x0, x^+1)$ – вероятность перехода из нуля в единицу; $P(x1) \cdot P(x^+0/x1) = P(x1, x^+0)$ – вероятность перехода из единицы в нуль.

2. ОПРЕДЕЛЕНИЕ СТАТИСТИЧЕСКОЙ НЕЗАВИСИМОСТИ СЛУЧАЙНЫХ БИТОВ

Условием статистической независимости генерируемых случайных битов является равенство всех условных вероятностей (7) или нулевое значение разности этих вероятностей: $\varepsilon(\tau) = 0$.

В экспериментальных измерениях понятие вероятности справедливо только для бесконечно большой последовательности случайных битов. Для ограниченной последовательности статистическим критерием независимости является попадание коэффициентов автокорреляционной функции в доверительный интервал $\pm 3\sigma$ с доверительной вероятностью $\alpha = 0{,}99$ [2].

В наших экспериментах длина последовательности выбиралась: $L_a = 1\,000\,000$ бит. С учетом соотношения (2) дисперсия автокорреляционной функции также равна: $D = L_a = 1\,000\,000$. Среднеквадратичное отклонение: $\sigma = \sqrt{D} = 1000$.

Поэтому при попадании коэффициентов автокорреляционной функции $K(\tau)$ в доверительный интервал ± 1000 можно утверждать о статистической независимости случайных битов с задержками, равной τ или более.

На рис. 4 приведены коэффициенты автокорреляционной функции, нормированные на величину среднеквадратичного отклонения $\sigma = 1000$. Скорость формирования случайных битов $Fo = 11$ МГц значительно превышает частоту шумовых импульсов диода с Зенеровским пробоем: $Fш = 3{,}8$ МГц.

Обратите внимание – форма графика напоминает известную функцию: $y = \sin(x) / x$. При величине задержки $\tau \geq 21$ все коэффициенты попадают в доверительный интервал ± 3, т.е. случайные биты, разнесенные на временной интервал: $t \geq 21 / Fo$, – не имеют корреляционных связей.

Аналогичные результаты получаются при исследовании влияния скорости формирования случайных последовательностей *Fo* на их статистические свойства.

На рис. 5 показаны экспериментальные зависимости коэффициентов автокорреляционной функции K(1), K(2) и K(3) (нормированных на величину среднеквадратичного отклонения $\sigma = 1000$) от безразмерного параметра: $m = Fш / Fo$.

Для коэффициента K(1) экспериментальная зависимость практически повторяет график на рис. 4 и условие статистической независимости соседних случайных битов (т.е попадание коэффициентов автокорреляционной функции в доверительный интервал $\pm 3\sigma$) наступает при скорости формирования *Fo* меньшей в 7,5 раз, чем частота шумовых импульсов *Fш* на выходе датчика (при $m_{кр} = Fш / Fo = 7{,}5$).

При величине $m = Fш / Fo = 1$ значение коэффициента автокорреляционной функции K(1) имеет отрицательное значение (см. рис. 5), потому что на вход счетного триггера T (см. рис. 1) за время формирования следующего бита поступает в среднем один случайный импульс от датчика шума и состояние счетного триггера изменяется на противоположное. Поэтому количество несовпадений соседних битов будет значительно больше, чем количество совпадений.

При величине $m = Fш / Fo = 2$ значение коэффициента K(1) имеет положительное значение, потому что на вход счетного триггера T за время формирования следующего бита поступает в среднем два случайных шумовых импульса и состояние счетного триггера после двух инверсий совпадает с предыдущим значением. Количество совпадений соседних битов будет значительно больше, чем несовпадений.

Аналогичные изменения знака коэффициента автокорреляционной функции K(1) происходят и для последующих четных и нечетных значений безразмерного параметра *m*.

График зависимости K(2) от *m* повторяет график для коэффициента K(1), но сжат влево по горизонтали в два раза. Поэтому условие статистической независимости наступает при большей в два раза скорости формирования случайных битов *Fo* или меньшем в два раза параметре *m* (на рис. 5 эти условия отмечены эллипсами в таблице).

Аналогично: график зависимости K(3) от *m* сжат по горизонтали в три раза и условие независимости наступает при трехкратной скорости формирования.

На основе анализа этих графиков можно утверждать: если скорость формирования случайных битов соответствует условию независимости для единичной задержки: $|K(1)| < 3\sigma$, то коэффициенты автокорреляционной функции с большими задержками также будут удовлетворять условию независимости.

3. ОБЪЕДИНЕНИЕ ПОТОКОВ НЕЗАВИСИМЫХ СЛУЧАЙНЫХ СИГНАЛОВ

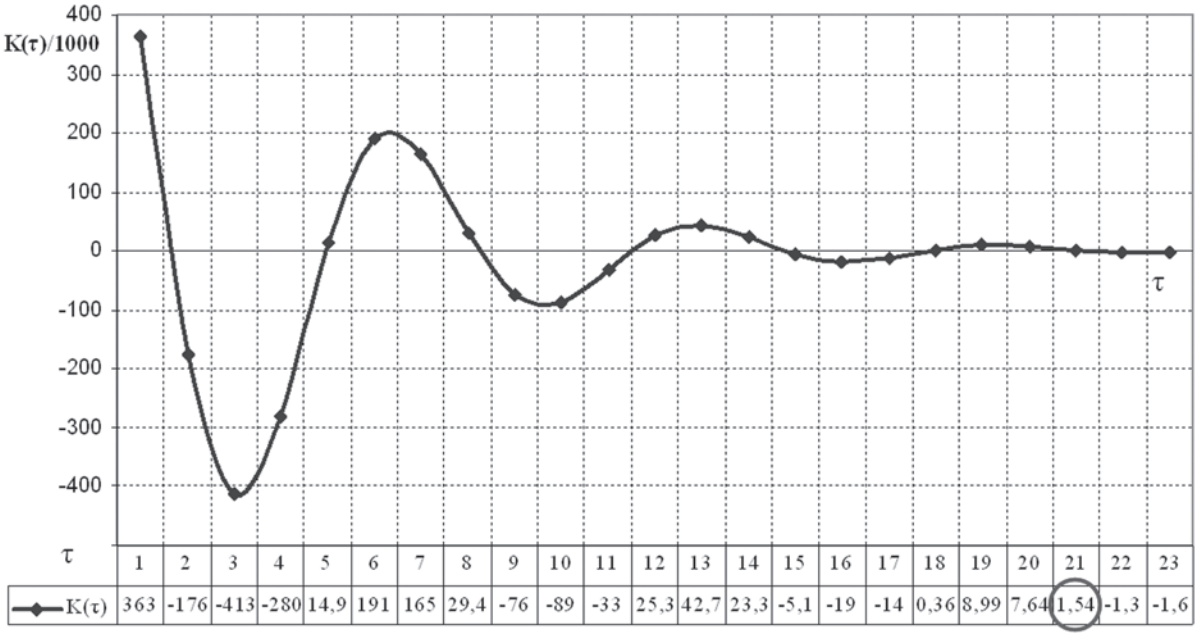
В патенте Украины № 61439 [3] предложено объединять логическим элементом XOR потоки независимых случайных сигналов (рис. 6), раздвинутых во времени многоразрядным сдвигающим регистром RG1.

Если у регистра RG1 только два отвода, то коэффициенты автокорреляционной функции для выходного случайного сигнала можно рассчитать по формуле (2):

$$K(\tau) = L_a - 2\sum(l_i \oplus l_{i+m}) \oplus (l_{i+\tau} \oplus l_{i+m+\tau}), \qquad (10)$$

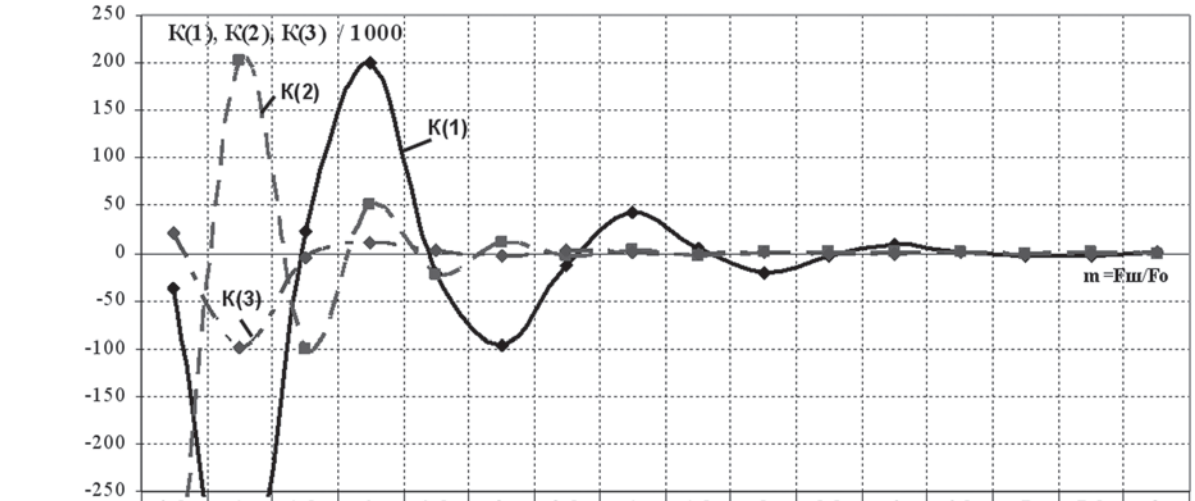
где: *m* – количество разрядов между отводами регистра.

В этой формуле учтено, что два случайных сигнала (сдвинутых во времени на количество



τ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
K(τ)	363	-176	-413	-280	14,9	191	165	29,4	-76	-89	-33	25,3	42,7	23,3	-5,1	-19	-14	0,36	8,99	7,64	1,54	-1,3	-1,6

Рис. 4. Коэффициенты автокорреляционной функции



m =Fш/Fo	0,5	1	1,5	2	2,5	3	3,5	4	4,5	5	5,5	6	6,5	7	7,5	8
K(1)	-37	-404	22,8	201	-21,2	-96	-12,1	43,2	5,8	-20,7	-3,9	8,1	0,8	-3,2	-2,1	0,8
K(2)	-389	203	-100	50,5	-23,7	10,4	-2,2	3	-2,2	1,5	0,1	0,4	0,8	-0,8	0,1	-0,4
K(3)	21	-97,8	-4,7	11,6	2,9	-2,7	2,4	1,5	-0,6	0,01	-1,1	-0,8	0,1	-0,7	-0,7	0,1

Рис. 5. Зависимости коэффициентов $K(1)$, $K(2)$ и $K(3)$ от безразмерного параметра: $m = Fш / Fo$.

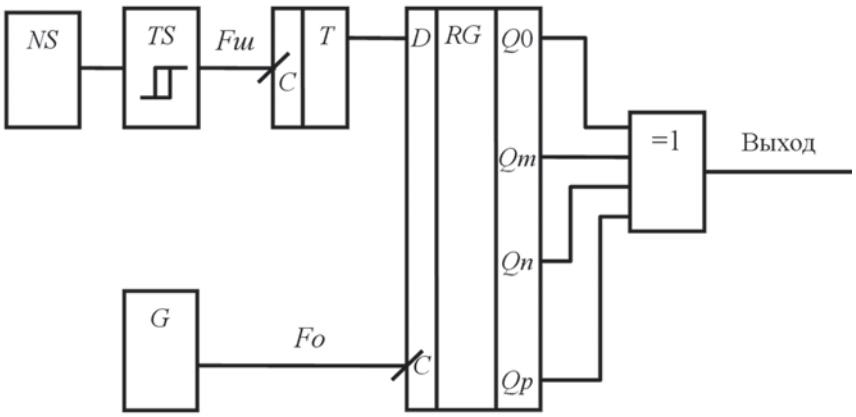


Рис. 6. Объединение независимых потоков случайных сигналов на отводах регистра элементом XOR

разрядов m) объединяются логическим элементом XOR и при вычислении коэффициентов автокорреляционной функции также используется сдвиг на количество разрядов τ с последующим объединением логической функцией XOR.

Используя сочетательный закон алгебры логики, уравнение (10) можно переписать в виде:

$$K(\tau) = L_a - 2\sum(l_i \oplus l_{i+\tau}) \oplus (l_{i+m} \oplus l_{i+m+\tau}). \quad (11)$$

В соответствии с этой формулой можно сначала рассчитать коэффициенты автокорреляционной функции отдельно для сигнала с первого отвода регистра (см. верхний ряд элементов сравнения на рис. 7), затем рассчитать коэффициенты автокорреляционной функции для сигнала со второго отвода (см. нижний ряд элементов сравнения на рис. 7), а потом «сложить по модулю 2» эти коэффициенты (см. средний ряд элементов сравнения на рис. 7).

Вероятности логических сигналов на выходах верхнего ряда (или нижнего ряда) элементов сравнения на рис. 7 равны:

$$P(0) = [P(x0) \cdot P(x^+0/x0) + P(x1) \cdot P(x^+1/x1)];$$

$$P(1) = [P(x0) \cdot P(x^+1/x0) + P(x1) \cdot P(x^+0/x1)].$$

Разность этих вероятностей в соответствии с уравнением (9) равна:

$$P(0) - P(1) = \varepsilon.$$

Поэтому можно записать: $P(0) = P(1) + \varepsilon$.

В табл. 1 приведены комбинации логических сигналов на входах логических элементов XOR для среднего ряда (см. рис. 7) и вероятности этих сигналов с учетом их статистической независимости.

Таблица 1

Входные сигналы		Вероятности
0	0	$[P(1) + \varepsilon] \cdot [P(1) + \varepsilon]$
0	1	$[P(1) + \varepsilon] \cdot P(1)$
1	0	$P(1) \cdot [P(1) + \varepsilon]$
1	1	$P(1) \cdot P(1)$

На выходах логических элементов XOR в среднем ряду (см. рис. 7) будет формироваться ло-

гический нуль при равенстве входных логических сигналов. Это соответствует первой и последней строкам в табл. 1.

Поэтому вероятность логического нуля на выходах элементов XOR равна:

$$P''(0) = [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] + P(1) \cdot P(1).$$

Выходная логическая единица на выходах элементов XOR в среднем ряду соответствует второй и третьей строке в табл. 1.

Вероятность логической единицы на выходах элементов XOR равна:

$$P''(1) = [P(1) + \varepsilon] \cdot P(1) + P(1) \cdot [P(1) + \varepsilon].$$

Разность вероятностей на выходе элементов XOR в среднем ряду численно равна нормированным коэффициентам автокорреляционной функции для схемы с объединением независимых потоков случайных сигналов на двух отводах сдвигающего регистра:

$$k'' = \varepsilon'' = P''(0) - P''(1) = [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] +$$
$$+P(1) \cdot P(1) - [P(1) + \varepsilon] \cdot P(1) - P(1) \cdot [P(1) + \varepsilon] = \varepsilon^2. \quad (12)$$

Из этого равенства следует: если нормированные коэффициенты автокорреляционной функции для исходного сигнала без объединения независимых потоков: $k(\tau) = \varepsilon(\tau)$ – меньше единицы, то квадрат этой величины будет еще значительно меньше.

В общем случае – при разных значениях коэффициентов автокорреляционной функции у объединяемых независимых потоков случайных сигналов – необходимо умножать эти коэффициенты отдельно для каждой задержки τ:

$$k''(\tau) = k_1(\tau) \cdot k_2(\tau). \quad (13)$$

В табл. 2 приведены комбинации логических сигналов для схемы с объединением трех отводов сдвигающего регистра трехвходовым элементом XOR (см. рис. 6) и вероятности этих сигналов с учетом их статистической независимости.

Таблица 2

Входные сигналы			Вероятности
0	0	0	$[P(1) + \varepsilon] \cdot [P(1) + \varepsilon] \cdot [P(1) + \varepsilon]$
0	0	1	$[P(1) + \varepsilon] \cdot [P(1) + \varepsilon] \cdot P(1)$
0	1	0	$[P(1) + \varepsilon] \cdot P(1) \cdot [P(1) + \varepsilon]$
0	1	1	$[P(1) + \varepsilon] \cdot P(1) \cdot P(1)$
1	0	0	$P(1) \cdot [P(1) + \varepsilon] \cdot [P(1) + \varepsilon]$
1	0	1	$P(1) \cdot [P(1) + \varepsilon] \cdot P(1)$
1	1	0	$P(1) \cdot P(1) \cdot [P(1) + \varepsilon]$
1	1	1	$P(1) \cdot P(1) \cdot P(1)$

Логический сигнал на выходе элемента XOR будет равен нулю при четном количестве входных единичных битов. Это соответствует первой, четвертой, шестой и седьмой строкам табл. 2. Вероятность логического нуля на выходе элемента XOR равна сумме вероятностей в этих строках.

Логическая единица на выходе элемента XOR соответствует второй, третьей, пятой и восьмой строкам табл. 2.

Нормированные коэффициенты автокорреляционной функции для каждой задержки τ численно равны разности этих вероятностей:

$$k'' = \varepsilon'' = [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] +$$
$$+[P(1) + \varepsilon] \cdot P(1) \cdot P(1) + P(1) \cdot [P(1) + \varepsilon] \cdot P(1) +$$
$$+ P(1) \cdot P(1) \cdot [P(1) + \varepsilon] - [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] \cdot$$
$$P(1) - [P(1) + \varepsilon] \cdot P(1) \cdot [P(1) + \varepsilon] - P(1) \cdot$$
$$\cdot [P(1) + \varepsilon] \cdot [P(1) + \varepsilon] - P(1) \cdot P(1) \cdot P(1) = \varepsilon^3. \quad (14)$$

Аналогично можно показать, что для схемы с объединением четырех отводов сдвигающего регистра четырехвходовым элементом XOR нормированные коэффициенты автокорреляционной функции численно равны :

$$k'' = \varepsilon'' = \varepsilon^4. \quad (15)$$

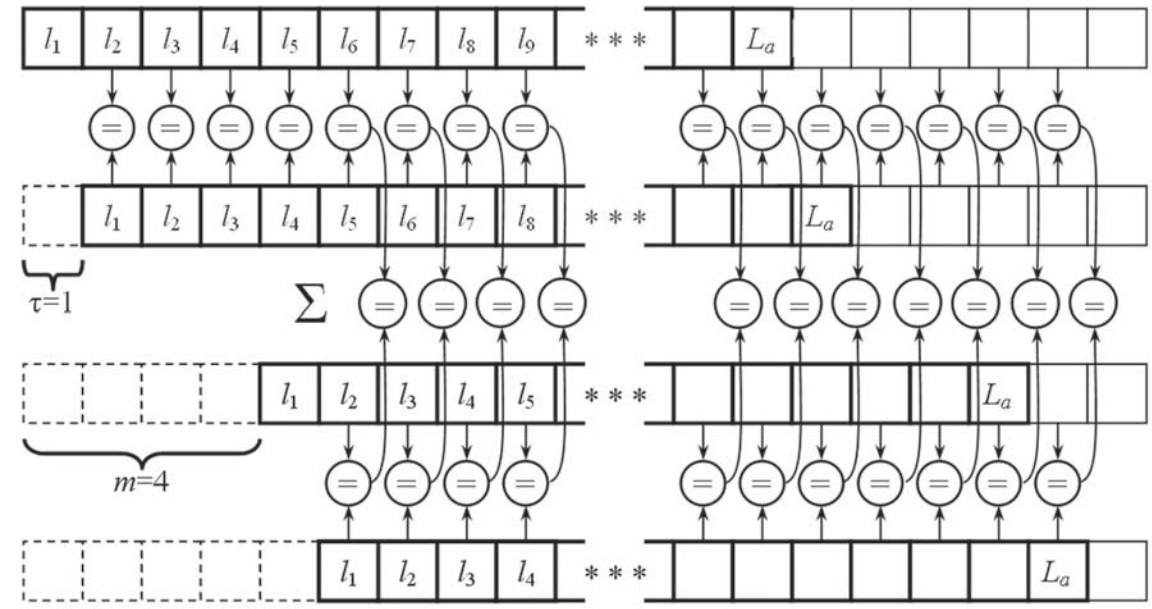


Рис. 7. Алгоритм вычисления автокорреляционной функции для регистра с объединением двух отводов элементом XOR

На рис. 8 приведены результаты измерений зависимости коэффициента автокорреляционной функции $K(1)$ от безразмерного параметра $m = Fш / Fo$ для исходного потока без объединений (график $n = 1$) и зависимости коэффициента $K(1)$ для объединения двух потоков элементом XOR ($n=2$), трех потоков ($n=3$) и четырех потоков ($n=4$) на отводах сдвигающего регистра (см. рис. 6).

Обратите внимание – коэффициенты $K(1)$ для регистра с двумя отводами ($n = 2$) имеют только положительные значения (в соответствии с уравнением (12)), и форма графика соответствует квадрату графика исходной зависимости ($n = 1$).

Нормированные значения коэффициентов автокорреляционной функции $k(1) = K(1) / D$ всегда меньше единицы. В наших экспериментах $D = L_a = 1\,000\,000$. Поэтому абсолютные значения в таблице в нижней части рис. 8 необходимо поделить на 1000.

Аналогично – форма графика для регистра с тремя отводами ($n = 3$) соответствует кубу исходной зависимости, а для графика ($n = 4$) форма соответствует четвертой степени графика исходной зависимости.

Полученные нормированные значения коэффициентов автокорреляционной функции соответствуют уравнениям (12), (14), (15).

Важный практический результат, полученный на основе анализа зависимостей коэффициентов автокорреляционной функции на рис. 8, – это возможность увеличения скорости формирования случайных битов (Fo) в два раза для регистра с двумя отводами (на рис. 8 условия независимости в таблице обведены окружностями).

Для схемы с тремя отводами и объединением случайных независимых потоков трехвходовым элементом XOR скорость формирования Fo можно увеличить в три раза при сохранении условия независимости всех формируемых случайных битов.

В общем случае можно утверждать: для схемы (рис. 6) с количеством отводов n можно увеличить скорость формирования в n раз.

При объединении элементом XOR статистически независимых потоков с различными автокорреляционными функциями их результирующие нормированные коэффициенты равны произведению исходных коэффициентов для каждой задержки τ. На рис. 9 показаны коэффициенты автокорреляционных функций для двух независимых сигналов: исходной схемы формирования случайных битовых последовательностей ($k_1(\tau)$) и схемы с детерминированными перестановками битов ($k_2(\tau)$) [4].

В соответствии с уравнением (13) для каждой задержки τ коэффициенты результирующей автокорреляционной функции $k''(\tau)$ меньше, чем наименьший из коэффициентов исходных автокорреляционных функций $k_1(\tau)$ или $k_2(\tau)$, потому что наименьший из коэффициентов умножается на число, меньшее единицы. Это утверждение справедливо для значений модуля коэффициентов автокорреляционных функций (без учета знака).

ВЫВОДЫ

На основе анализа результатов исследований автокорреляционных функций выходных сигналов АГСП с датчиками шума на основе кремниевых диодов с Зенеровским пробоем можно сделать следующие выводы:

• Условием статистической независимости генерируемых случайных битов является равенство всех условных вероятностей переходов соседних случайных битов или нулевое значение разности этих вероятностей: $\varepsilon(\tau) = 0$;

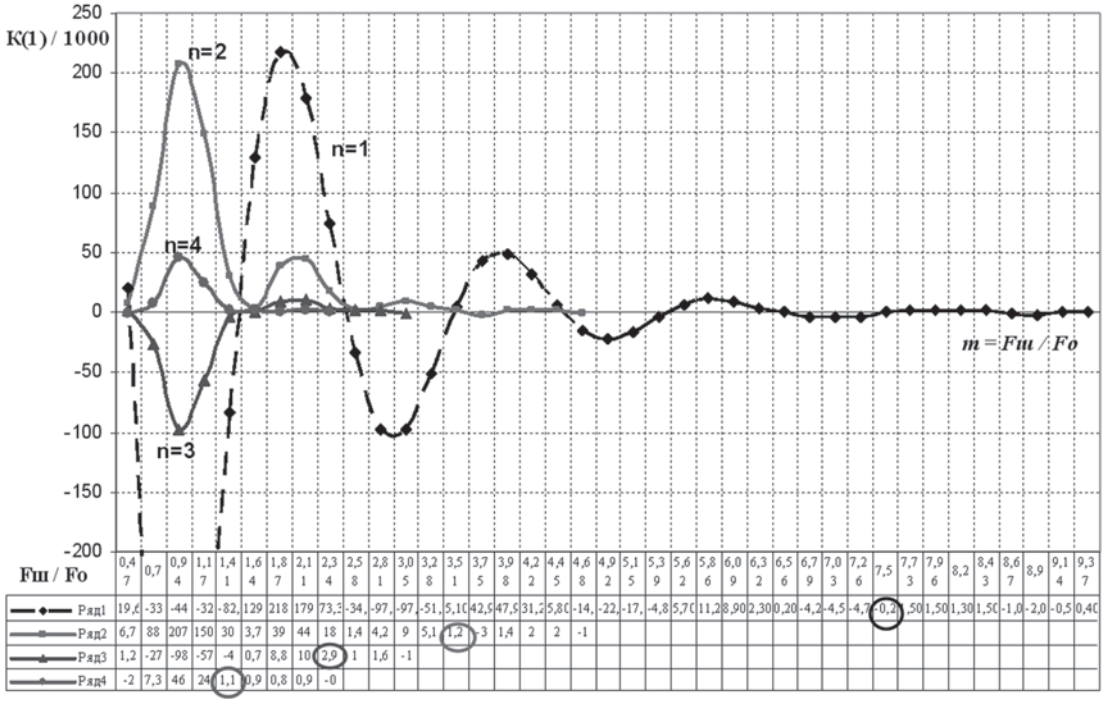


Рис. 8. Зависимости коэффициентов автокорреляционной функции $K(1)$ для регистра с отводами

Рис. 9. Нормированные автокорреляционные функции для сигналов с объединением элементом XOR

• Для ограниченной последовательности случайных битов статистическим критерием независимости является попадание коэффициентов автокорреляционной функции в доверительный интервал $\pm 3\sigma$ с доверительной вероятностью $\alpha = 0{,}99$;

• Объединение потоков независимых случайных последовательностей элементом XOR (сумматором по модулю 2) уменьшает модули нормированных коэффициентов автокорреляционных функций и, в конечном итоге, позволяет повысить скорость формирования случайных последовательностей.

Литература.

[1] *А.А. Торба, С.Г. Елаков, А.З. Степченко.* Генерация равновероятных случайных последовательностей на основе физических датчиков // Радиотехника. Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119, с.108-113.

[2] *А. Менезис, П. ван Оршоа, С. Ватсон,* Руководство по прикладной криптографии – CRC: Press, 1996. – 816 с.

[3] Декларационный патент Украины № 61439 А, Бюл. № 11 от 17.11.2003.

[4] Патент Украины № 86979, Бюл. № 11 от 10.06.2009.

Поступила в редколлегию 22.06.2010.

Торба Александр Алексеевич, кандидат технических наук, доцент кафедры ЭВМ ХНУРЭ. Область научных интересов: аппаратные средства криптографических систем.

Бобух Всеволод Анатольевич, кандидат технических наук, начальник отдела аппаратных средств защиты информации ЗАО «ИИТ», старший научный сотрудник кафедры БИТ ХНУРЭ. Область научных интересов: апаратные средства систем защиты информации.

Торба Анна Александровна, ассистент кафедры ПО ЭВМ, ХНУРЭ. Область научных интересов: аппаратно-программные средства криптографических систем.

УДК 681.324.067

Аналіз автокореляційних функцій випадкових сигналів / А.А. Торба, В.А. Бобух, Г.О. Торба // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 411-417.

У статті було розглянуто результати експериментальних досліджень апаратних генераторів випадкових послідовностей та їх автокореляційних функцій.

Ключові слова: автокореляційна функція, апаратний генератор випадкових послідовностей.

Табл. 02. Іл.09. Бібліогр.: 04 найм.

UDC 681.324.067

Analysis of autocorrelation functions of random signals / A.A. Torba, V.A. Bobukh, A.A. Torba // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 411-417.

Results of experimental researches of hardware generators of random sequences and their autocorrelation functions are considered in the paper.

Key words: autocorrelation function, hardware random sequences generator.

Tab. 02. Fig. 09. Ref.: 04 items.