Прикладные задачи нелинейной теории колебаний и волн

Изв. вузов «ПНД», т. 17, № 6, 2009 УДК 621.373.54, 517.9

# ЦИФРОВОЙ ГЕНЕРАТОР ПОДКАЧКИ ЭНТРОПИИ НА БАЗЕ ОТОБРАЖЕНИЯ АРНОЛЬДА

*Л.С. Сотов, В.Н. Харин*

В работе обсуждается использование цифровых генераторов, моделируемых двумерными отображениями на торе, в частности отображением «Кот Арнольда», в качестве встроенных источников энтропии, работающих в составе однокристальных криптографических систем генерации случайных чисел. Приводится практическая схема генератора на двоичных счетчиках, реализуемая на стандартной элементной базе фабрик – производителей полупроводников. Проводится сравнительная характеристика генераторов подкачки энтропии. Анализируются условия безопасности их использования.

*Ключевые слова:* Генератор случайных чисел, динамический хаос, источники энтропии, криптографические ключи, распределение вероятностей.

Большинство систем информационной безопасности имеют в своем составе генераторы случайных чисел. В связи с тем, что к данным генераторам предъявляются жесткие технические требования, использование непосредственно физических источников случайных сигналов, таких как тепловые, дробовые шумы в электронных схемах, процессы разряда в счетчиках Гейгера и т.п. обычно не представляется возможным [1,2]. Для генерации случайных чисел используются криптографические генераторы псевдослучайных последовательностей (ПСП). Для устранения угрозы восстановления последовательности по определенному в некоторый момент времени состоянию генератора ПСП периодически или по запросу системы в состояние генератора вносится неопределенность. При этом используются внешние источники случайных сигналов. Вопросы их получения и использования являются актуальными в настоящее время [3]. В литературе по криптографии такие источники часто называют источниками подкачки энтропии в систему [2]. Для большинства систем использование внешних источников случайных сигналов недопустимо из соображений безопасности, поэтому используются встроенные в систему безопасности генераторы случайных сигналов (ГСС).

Возможны два подхода при построении ГСС для подкачки энтропии.

1. Использование ГСС, работающих на флуктуациях параметров в системах с большим числом степеней свободы. При этом используется «мощный источник энтропии», а необходимый уровень сигнала получают путем его усиления.

2. Построение ГСС на базе систем с хаотической динамикой. При этом используется «слабый источник энтропии», например, обычный генератор тактовых импульсов, а динамическая система служит в качестве усилителя неопределенности.

Недостатком ГСС, работающих путем усиления случайных сигналов, таких как тепловые, дробовые шумы в электронных схемах и т.п., является малая среднеквадратичная мощность естественных флуктуаций. Это приводит к необходимости использования высокочувствительных усилителей с большим коэффициентом усиления и делает данную схему уязвимой к воздействиям со стороны злоумышленника. Высокочувствительные входные каскады усилителей имеют низкий порог насыщения. Злоумышленник может преднамеренно наводить помехи, переводящие усилитель естественных флуктуаций в режим насыщения, блокируя, таким образом, работу ГСС. В целях обеспечения безопасности представляет интерес использование динамических ГСС, которые построены на базе динамических систем с хаотической динамикой. Возможно совместное использование в качестве источников подкачки энтропии генераторов, работающих на основе систем с хаотической динамикой и с усилением естественных флуктуаций.

Известно большое количество радиотехнических генераторов с хаотической динамикой, однако большинство из них содержат либо нестандартные нелинейные элементы, либо элементы, не реализуемые в составе интегральной микросхемы (катушки индуктивности, конденсаторы достаточно большой емкости и.п.). Кроме того, для обеспечения безопасности использования такого генератора в составе используемой системы необходимо, чтобы характер его колебаний не менялся при внешних воздействиях, которые могут быть достаточно интенсивны.

С технической стороны проектируемый генератор должен удовлетворять следующим требованиям:

– ГСС должен соответствовать модели безопасности, используемой при разработке аппаратуры [2];

– должна быть обеспечена простота и надежность схемотехнических решений, а также некритичность требований к элементной базе (нестандартные элементы в ГСС не используются).

В данной работе предлагается использовать в качестве ГСС цифровой генератор, моделируемый двумерным линейным отображением на торе. Отличительной особенностью данного генератора является простота и возможность реализации в виде встроенной системы на кристалле, без предъявления каких-либо дополнительных требований к элементной базе производителя.

## Модель безопасности использования ГСС

Сформулируем условия безопасности использования ГСС в криптографических системах генерации случайных чисел. На рис. 1 схематически изображена блок-схема, иллюстрирующая модель ГСС, работающего во враждебной среде. Злоумышленник может воздействовать на ГСС и анализировать данные о его состоянии в различные моменты времени, используя доступные технические каналы утечки информации [4]. Кроме этого злоумышленнику известна конструкция и алгоритмы работы ГСС, так что он может моделировать его работу. По запросу системы

в некоторые моменты времени $T_i$ на основе внутреннего состояния $\vec{X}(T_i)$ генератора формируется цифровой сигнал $\{DS\}_{T_i}$, который по некоторому алгоритму вносит неопределенность в состояние генератора ПСП. Система определяет $\vec{X}(T_i)$ с погрешностью δ, таким образом $\{DS\}_{T_i}$ генерируется на основе любого значения $\vec{X}$из δ-окрестности $\vec{X}(T_i)$ в фазовом пространстве системы $\{\vec{X}\}^{\delta}_{T_i} = \{\vec{X} : \forall\vec{X},\ \left|\vec{X} - \vec{X}(T_i)\right| < \delta\}$.

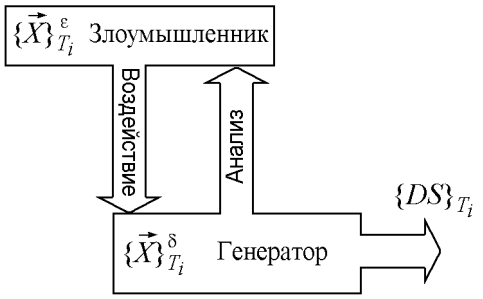



Рис. 1. Модель генератора случайных сигналов, работающего во враждебной среде

Цифровой сигнал $\{DS\}_{T_i}$ генерируется системой по известному злоумышленнику алгоритму $s$ для $\forall\vec{X}(T_i) \in \{\vec{X}\}^{\delta}_{T_i},\ \ s(\vec{X}(T_i)) \to \{DS\}_{T_i}$.

Целью злоумышленника является определение состояния$\vec{X}(T_i)$ с погрешностью, не превышающей δ. ГСС будет безопасным, если злоумышленник не может определить состояние ГСС в требуемые моменты времени $T_i$ с необходимой точностью даже в том случае, если некоторые значения из последовательности $\vec{X}(T_i)$ ему известны.

Пусть $\varepsilon > 0$ – погрешность определения злоумышленником состояния динамической системы $\vec{X}(T_i)$. Объем фазового пространства $\{\vec{X}\}^{\varepsilon}_{T_i} = \{\vec{X} : \forall\vec{X},\ \left|\vec{X}-\vec{X}(T_i)\right| < \varepsilon\}$ известен злоумышленнику, $\{\vec{X}\}^{\delta}_{T_i} \in \{\vec{X}\}^{\varepsilon}_{T_i}$. Если рассматривать $\{X\}^{\varepsilon}_{T_i}$ как множество, содержащее непересекающиеся подмножества $\{\vec{X}\}^{\delta}_{T_i}$, то $\{X\}^{\varepsilon}_{T_i} = \{\ \{\vec{X}_1\}^{\delta}_{T_i}, \{\vec{X}_2\}^{\delta}_{T_i}, ..., \{\vec{X}_L\}^{\delta}_{T_i}\}$. Пусть мощность $M\{X\}^{\varepsilon}_{T_i} = L$. Величина $L$ определяет уровень безопасности ГСС. Если $L$ больше значения $L_m$, определенного разработчиком в качестве параметра модели безопасности данной системы, использование ГСС безопасно [2].

При использовании безопасного ГСС для злоумышленника также вычислительно неразрешимы задачи уточнения состояния ГСС путем анализа временной эволюции. Это условие выполняется в случае локальной неустойчивости траекторий аттрактора в фазовом пространстве ГСС.

Оценим возможности злоумышленника по уточнению состояния ГСС по известным фрагментам $\vec{X}(T_i)$.

Пусть моделью ГСС является дискретное отображение

$$\vec{X}_{n+1} = \vec{F}(\vec{X}_n). \tag{1}$$

$\vec{X}^{\xi}_n = \vec{X}_n + \vec{\xi}_n$ – близкая к $\vec{X}_n$ траектория в фазовом пространстве ГСС. Тогда, учитывая малость $\left|\vec{\xi}_n\right|$ и линеаризуя уравнение (1) вблизи траектории $\vec{X}_n$ в фазовом пространстве ГСС, получим уравнение для $\vec{\xi}_n$

$$\vec{X}^{\xi}_{n+1} = \vec{F}(\vec{X}_n + \vec{\xi}_n) = \vec{F}(\vec{X}_n) + \left[A(\vec{X}_n)\right]\vec{\xi}_n,$$
$$\vec{\xi}_{n+1} = \left[A(\vec{X}_n)\right]\vec{\xi}_n,$$

где $\left[A(\vec{X}_n)\right]$ – матрица Якоби для $\vec{F}(\vec{X}_n)$.

Рассмотрим эволюцию $\left|\vec{\xi}_n\right|^2 = \vec{\xi}_n^{\mathrm{T}}\vec{\xi}_n$, где $\vec{\xi}_n^{\mathrm{T}}$ – транспонированный вектор начальных возмущений $\vec{\xi}_n$

$$\left|\vec{\xi}_{n+1}\right|^2 = \vec{\xi}_n^{\mathrm{T}}\left[A(\vec{X}_n)\right]^{\mathrm{T}}\left[A(\vec{X}_n)\right]\vec{\xi}_n,$$

где $\left[A(\vec{X}_n)\right]^{\mathrm{T}}$ – транспонированная матрица $\left[A(\vec{X}_n)\right]$.

Рассмотрим матрицу $\left[\nu(\vec{X}_n)\right] = \left[A(\vec{X}_n)\right]^{\mathrm{T}} \times \left[A(\vec{X}_n)\right]$. Собственные значения $\chi_s$ и собственные векторы $\vec{H}_s$ этой матрицы находятся из уравнения

$$\left[\nu(\vec{X}_n)\right]\vec{H}_s = \chi_s\vec{H}_s. \tag{2}$$

Задавая малое возмущение $\vec{\xi}_n$ вдоль одного из собственных векторов $\vec{H}_s$, получим

$$\left|\vec{\xi}_{n+1}\right|^2 = \vec{\xi}_n^{+}\left[A(\vec{X}_n)\right]^{\mathrm{T}} \times \left[A(\vec{X}_n)\right]\vec{\xi}_n = \chi_s\left|\vec{\xi}_n\right|^2,$$

$$\frac{\left|\vec{\xi}_{n+1}\right|}{\left|\vec{\xi}_n\right|} = \sqrt{\chi_s}. \tag{3}$$

Начальное малое возмущение будет возрастать, если $\chi_s > 1$. Если начальное возмущение возрастает для любого $n$, то ГСС безопасен для анализа в прямом времени по любому участку фазовой траектории, поскольку при попытках моделировать динамику генератора погрешность определения его состояния будет возрастать. Если отображение (1) необратимо, условием безопасности ГСС является $\chi_s > 1$для любого $\vec{X}_n$. Наличие положительного показателя Ляпунова отображения (1) является менее строгим требованием, поскольку на аттракторе системы возможны участки локально-устойчивых последовательностей $\vec{X}_k$, анализируя которые злоумышленник может уточнить состояние ГСС.

Если отображение (1) обратимо, злоумышленник может инвертировать время и попытаться уточнить состояние ГСС путем моделирования отображения, обратного (1)

$$\vec{\xi}_n = \left[A(\vec{X}_n)\right]^{-1}\vec{\xi}_{n+1}. \tag{4}$$

Аналогично получаем

$$\left[\nu(\vec{X}_n)\right]^{-1} = \left(\left[A(\vec{X}_n)\right]^{-1}\right)^{\mathrm{T}} \times \left[A(\vec{X}_n)\right]^{-1},$$

$$\left(\left[A(\vec{X}_n)\right]^{-1}\right)^{\mathrm{T}} \times \left[A(\vec{X}_n)\right]^{-1}\vec{H}_s = \chi_s^r\vec{H}_s,$$

$$\frac{1}{\chi_s^r}\vec{H}_s = \left[A(\vec{X}_n)\right]\left[A(\vec{X}_n)\right]^{\mathrm{T}}\vec{H}_s = \left[A(\vec{X}_n)\right]^{\mathrm{T}}\left[A(\vec{X}_n)\right]\vec{H}_s = \left[\nu(\vec{X}_n)\right]\vec{H}_s.$$

Таким образом, $\chi_s = 1/\chi_s^r$, и ГСС будет безопасным для анализа в обратном времени, если одно из собственных значений $\chi_s < 1$.

Следовательно, если моделью ГСС является дискретное отображение, и в спектре собственных значений всех матриц малых возмущений $\left\{[\nu(\vec{X}_n)],\ n = 1, 2, ..., \infty\right\}$ есть хотя бы одно $\chi_s > 1$ и $\chi_s < 1$, ГСС является безопасным по отношению к попыткам уточнить его состояние путем вычислений по известной с погрешностью $\varepsilon$ временной последовательности $\vec{X}_n$

$$\forall \left[\nu(\vec{X}_n)\right]\ \ \exists s : \chi_s > 1 \& \ \exists q : \chi_q < 1. \tag{5}$$

Менее строгим требованием безопасности является наличие хотя бы одного положительного и одного отрицательного показателя Ляпунова отображения (1).

Учитывая возможность внешнего воздействия на ГСС с целью изменения режима работы, необходимо, чтобы условие (5) сохранялось при любом возможном внешнем воздействии.

## Модель цифрового ГСС

Эффективная техническая реализация ГСС в цифровой системе возможна на базе модельного отображения на торе [5]

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a_{11}a_{12} \\ a_{21}a_{22} \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod(1). \tag{6}$$

Из класса отображений, задаваемых уравнением (6), далее будут рассматриваться отображения, сохраняющие площадь $a_{11}a_{22} - a_{12}a_{21} = 1$ и являющиеся отображениями гиперболического типа: $(a_{11}+a_{22}) > 2$; $a_{11}+a_{22}+\sqrt{(a_{11}+a_{22})^2-4} > 1$; $a_{11}+a_{22}-\sqrt{(a_{11}+a_{22})^2-4} < 1$. Эти условия являются достаточными для безопасности ГСС в рассмотренном ранее смысле.

В цифровых системах в качестве непрерывных переменных $(x, y)$ удобно использовать длительность генерируемых импульсов. Импульс длительности $\tau$ можно формировать с использованием реверсивного двоичного счетчика $\tau = n\tau_g$, где $n$ – двоичное число, загружаемое в счетчик, $\tau_g$ – период следования тактовых импульсов, подаваемых на счетчик. Двоичный счетчик разрядности $N$ осуществляет счет по модулю $2^N$. Поэтому при использовании в ГСС счетчиков перепишем (6) для целочисленных переменных $(k, m)$:

$$\begin{pmatrix} k_{n+1} \\ m_{n+1} \end{pmatrix} = \begin{pmatrix} a_{11}a_{12} \\ a_{21}a_{22} \end{pmatrix} \begin{pmatrix} k_n \\ m_n \end{pmatrix} \bmod(2^N). \tag{7}$$

Переход от (6) к (7) равносилен потере точности вычислений переменных $(x, y)$, которые определяются с погрешностью $2^{-N}$. Отображения (6) и (7) можно считать эквивалентными для достаточно больших $N$, учитывая, однако, что из-за конечности множества целых чисел, на котором задано отображение (7), последнее будет периодическим с периодом не более $2^N$.

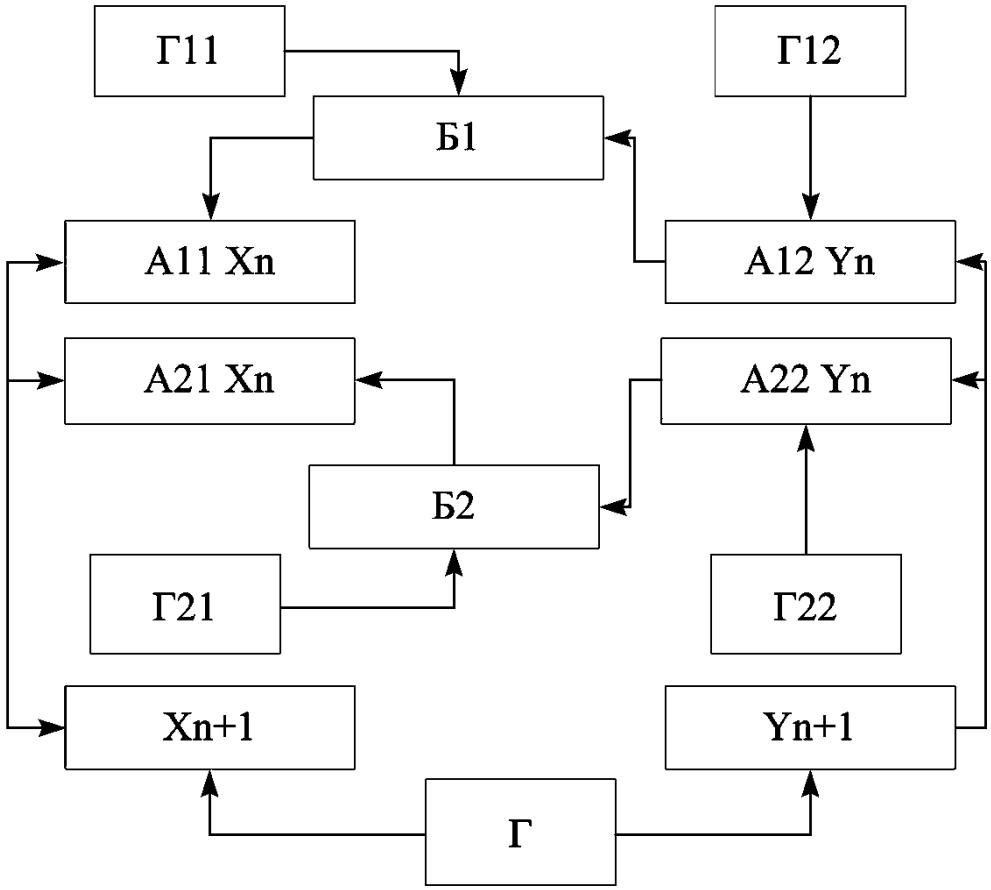



Рис. 2. Блок-схема ГСС на двоичных счетчиках

Построение цифрового ГСС, в котором реализуется модельное отображение Арнольда возможно на двоичных счетчиках. На рис. 2 представлена блок-схема разработанного ГСС. Моделирование архитектуры данного генератора выполнено на языке SystemC на уровне регистров и каналов передачи данных (RTL уровень) [6]. В процессе работы ГСС вырабатывает импульсы с длительностью, определяемой приведенным ниже выражением (8).

В общем случае ГСС состоит из четырех $N$-разрядных реверсивных двоичных счетчиков A11Xn, A12Yn, A21Xn, A22Yn, двух обычных двоичных счетчиков Xn+1, Yn+1 и, в общем случае, пяти генераторов тактовых импульсов Г, Г11, Г12, Г21, Г22, а также логических блоков Б1 и Б2, пропускающих импульсы от соответствующих генераторов Г11, Г21 при обнулении счетчиков A12Yn, A22Yn, соответственно. Данную схему можно реализовать только на цифровых элементах, используя в качестве Г, Г11, Г12, Г21, Г22 быстродействующие автогенераторы, частота колебаний которых определяется инерционными свойствами используемых логических элементов [7]. Если $\tau_g$ – период следования тактовых импульсов, подаваемых на генератор Г, то $\tau_{11} = a_{11}\tau_g$, $\tau_{12} = a_{12}\tau_g$, $\tau_{21} = a_{21}\tau_g$, $\tau_{22} = a_{22}\tau_g$ – периоды следования тактовых импульсов генераторов Г11, Г12, Г21, Г22, соответственно. Соотношение частот генераторов тактовых импульсов определяет коэффициенты отображения (6) и в конечном итоге характер динамики генератора.

В начальный момент времени счетчики Xn+1, Yn+1 обнуляются, в A11Xn, A21Xn заносится начальное значение $k_0$, а в счетчики A12Yn, A22Yn заносится значение $m_0$. После этого тактовые импульсы от генераторов Г, Г12, Г22 подаются на соответствующие счетчики Xn+1, Yn+1, A12Yn, A22Yn, причем A12Yn, A22Yn осуществляют реверсивный счет, а Xn+1, Yn+1 – прямой. После обнуления счетчиков A12Yn, A22Yn тактовые импульсы от генераторов Г11, Г21 через логические схемы Б1 поступают на счетчики A11Xn, A21Xn, осуществляющие реверсивный счет. Цикл завершается в момент обнуления этих счетчиков. Для осуществления следующего цикла содержимое счетчиков Xn+1, Yn+1 записывается в A11Xn, A21Xn и A12Yn, A22Yn, соответственно. Время, необходимое для совершения цикла по элементам $k - T^k_{n+1} = k_{n+1}\tau_g = (a_{11}k_n + a_{12}m_n)\tau_g$; время, необходимое для совершения цикла по элементам $m - T^m_{n+1} = m_{n+1}\tau_g = (a_{21}k_n + a_{22}m_n)\tau_g$. Используя матричную запись, уравнения можно переписать в виде

$$\begin{pmatrix} T^k_{n+1} \\ T^m_{n+1} \end{pmatrix} = \begin{pmatrix} a_{11}a_{12} \\ \\ a_{21}a_{22} \end{pmatrix} \begin{pmatrix} T^k_n \\ T^m_n \end{pmatrix} \bmod(2^N\tau_g). \tag{8}$$

Учитывая флуктуации периодов колебаний генераторов Г, Г11, Г12, Г21, Г22, длительности циклов $T^k_n, T^m_n$ являются случайными величинами. Если флуктуации периодов колебаний генераторов – независимые случайные величины, распределение $T^k_n, T^m_n$ будет нормальным:

$$\rho(T^k_n, T^m_n) = \frac{1}{2\pi km\sigma}\ \exp\left(\frac{(T^k_n - \mu(T^k_n))^2}{2k^2\sigma^2} + \frac{(T^m_n - \mu(T^m_n))^2}{2m^2\sigma^2}\right). \tag{9}$$

Здесь σ – дисперсия периодов поступающих на счетчик импульсов; $\mu(T^k_n)$ и $\mu(T^m_n)$ – математические ожидания длительностей циклов $T^k_n$ и $T^m_n$; $k$, $m$ – число импульсов, которое поступило на двоичные счетчики за время $T^k_n$ и $T^m_n$, соответственно. Поскольку $k_n = \dfrac{T^k_n}{\tau_g}, m_n = T^m_n/\tau_g$, целочисленные величины $(k_n, m_n)$ отображения (7) станут случайными. Полагая, что $\mu(\tau_g)$ – математическое ожидание $\tau_g$,

$$P(k_n, m_n) = \int_{m_n\mu(\tau_g)}^{(m_n+1)\mu(\tau_g)} \int_{k_n\mu(\tau_g)}^{(k_n+1)\mu(\tau_g)} \rho(T^k_n, T^m_n) dT^k_n dT^m_n. \tag{10}$$

Преобразование (8) вследствие гиперболичности системы приводит к росту энтропии $S$ в системе. С каждым циклом отображения (7) неопределенность в системе возрастает. Рассмотрим процесс роста $S$ для $(k_n, m_n)$. Пусть $\vec{H}_1, \vec{H}_2$ – собственные векторы, а $\chi_1 > 1$, $\chi_2 < 1$ – собственные значения матрицы $[A] = \begin{pmatrix} a_{11}a_{12} \\ a_{21}a_{22} \end{pmatrix}$. Вдоль $\vec{H}_1$ происходит растяжение, вдоль $\vec{H}_2$ – сжатие. На рис. 3 представлена эволюция плотности распределения (9) при итерациях отображения Арнольда $[A] = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ для $n = 0, 1, 2, 3$. Вследствие сжатия вдоль направления $\vec{H}_2$ двумерная плотность распределения быстро приближается к одномерной,

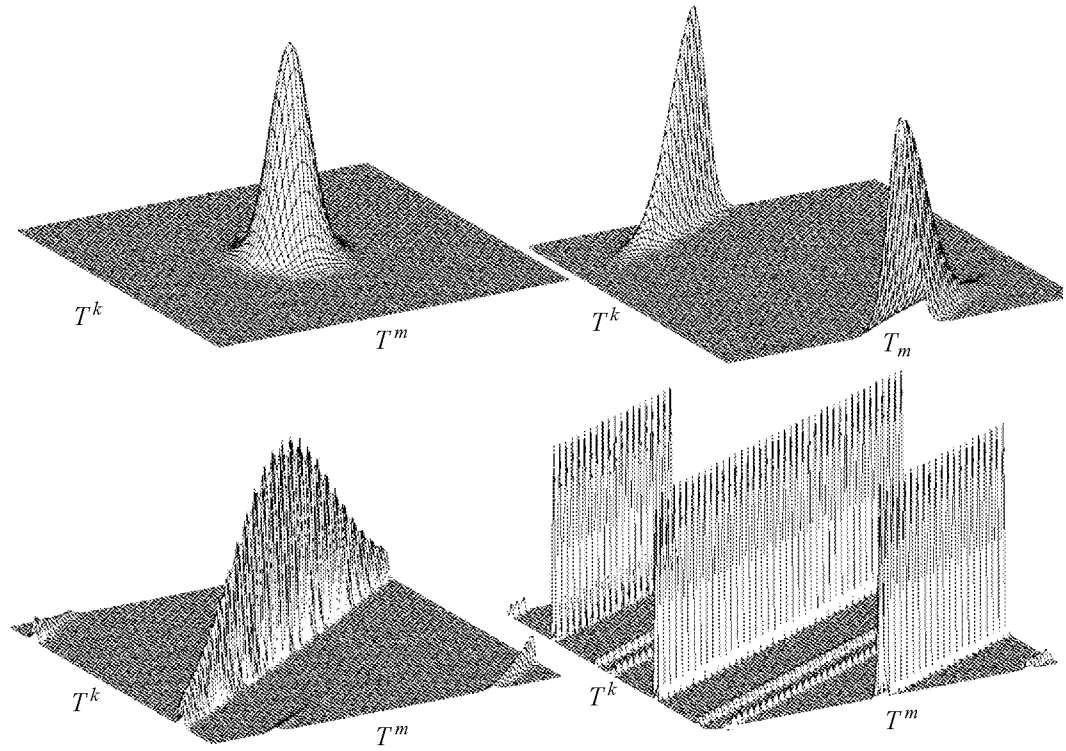



Рис. 3. Эволюция функции распределения плотности вероятности периода ГСС

и поверхность заполняется листами «всплесков» плотности вероятности. Частоты генераторов Г, Г11, Г12, Г21, Г22 необходимо выбирать так, чтобы обеспечить иррациональность углового коэффициента линии, вдоль которой расположен вектор $\vec{H}_1$ [5]. В этом случае листы не перекрываются, а плотно заполняют всю поверхность, и энтропия, накапливаемая системой, будет максимальна: $S_{\max} = 2N$.

Вследствие растяжения вдоль направления $\vec{H}_1$ энтропия системы $S_n = -\sum_{k=1}^{N}\sum_{m=1}^{N} P(k_n, m_n)\log_2 P(k_n, m_n)$ растет линейно с шагом $\Delta S = l\log_2\chi_1$ за каждую итерацию (7). При среднем времени выполнения цикла $T_g \approx 2^{N-1}\tau_g$ производительность генератора в качестве источника энтропии $P_S = (1/T_g)l\log_2\chi_1$. Накопление максимальной энтропии происходит за $L = (2N)/(\log_2\chi_1)$ циклов, на которое затрачивается $T_L = (2NT_g)/(\log_2\chi_1) \approx (N2^N\tau_g)/(\log_2\chi_1)$ времени. Если в некоторый момент времени стало известно состояние счетчиков ГСС, то за каждый цикл работы генератора происходит потеря информации о текущем состоянии $\Delta I = l\log_2\chi_1$ [8]. Эффективным путем увеличения производительности генератора энтропии является сокращение $T_g$, менее эффективным – увеличение $\chi_1$.

Минимальная разрядность счетчиков определяется из соотношения $N > \log_2(\tau_g/\sigma)$. Оценим практическое число разрядов двоичных счетчиков и среднюю длительность цикла ГСС. Пусть генератор Г работает на частоте $f_0 = 100$ МГц, и его нестабильность определяется значением $\sigma = 10^{-4}$. В этом случае необходимо обеспечить $N > 13$ (при $N = 14$ средняя длительность цикла $T_g$ будет около 164 мкс).

## Выводы

В работе предложена модель безопасности использования ГСС в системах генерации случайных чисел. Приведена архитектурная модель генератора импульсов случайной длительности с использованием только стандартных цифровых логических элементов, которая выполнена на уровне регистров и передачи данных. Динамика изменения длительности импульсов данного ГСС определяется двумерным отображением типа отображения Арнольда. Генератор удовлетворяет сформулированным в работе требованиям безопасности. Проведена оценка роста энтропии в системе и получено соотношение для минимальной разрядности используемых двоичных счетчиков. Данный генератор не обладает высоким быстродействием, однако, его быстродействия достаточно для применения данного генератора в качестве источника подкачки энтропии в криптографических системах генерации случайных чисел. Генератор прост, не требует наладки и может быть встроен в проектируемые системы на кристалле (SoC) или программируемую логическую матрицу (FPGA) путем проведения процедуры логического синтеза.

Если предположить возможность преднамеренного воздействия со стороны злоумышленника на ГСС, работающий за счет усиления естественных флуктуаций, возможно блокирование его функций за счет наводок на высокочувствительные входные каскады усилителей. В этом случае предпочтительно использование подхода, при котором используются «слабый источник энтропии», например, флуктуации периода колебаний обычного генератора тактовых импульсов, и динамическая система с хаотической динамикой, которая служит в качестве усилителя неопределенности.

## Библиографический список


1. *Menezes A., van Oorschot P., Vanstone S.* Handbook of applied cryptography CRC, 1997. P. 39.
2. *Фергюсон Н., Шнайер Б.* Практическая криптография/ Пер. с англ. М.: Издательский дом «Вильямс», 2005. С. 34,35,56,57,178–209.
3. *Kelsey J., Schneier B., Wagner D. and Hall C.* Cryptanalytic attacks on pseudorandom number generators // Fast Software Encryption. 5th International Workshop, FSE'98. Lecture Notes in Computer Science. Springer-Verlag. 1998. Vol. 1372. P. 168.
4. *Куприянов А.М.* Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И.Куприянов, А.В.Сахаров, В. А. Шевцов. М.: Издательский центр «Академия», 2006. С. 48.
5. *Кузнецов С.П.* Динамический хаос. М.: ФИЗМАТЛИТ, 2001. 296 с.
6. *Евтушенко Н.Д., Немудров В.Г., Сырцов И.А.* Методология проектирования систем на кристалле. Основные принципы, методы, программные средства // «Электроника». 2003. № 3.
7. *Опадчий Ю.Ф., Глудкин О.П., Гуров А.И.* Аналоговая и цифровая электроника. М.: «Горячая Линия – Телеком». 2000. С. 681, 682
8. *Шустер Г.* Детерминированный хаос: Введение. М.: Мир, 1988. С. 115.



*Поступила в редакцию 12.01.2009*
*После доработки 3.04.2009*

## DIGITAL GENERATOR OF PUMPING OF ENTROPY ON THE BASIS OF ARNOLD'S MAPPING

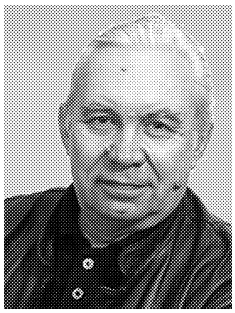
*L.S. Sotov, V.N. Harin*

The digital generators model-based by two-dimensional mappings on toroid, in particular by mapping «Arnold's Cat», as the built-in sources of entropy working as a part of single-crystal cryptographic systems of generation of random numbers is discussed. The practical scheme of the generator on the binary counters, realised on element base of semiconductor factories is resulted. The comparative characteristic of pumping of entropy generators is discussed. Safety conditions are analyzed.

*Keywords:* Random number generator, chaotic dynamics, entropy input streams, cryptographic keys, probability distribution.

*Сотов Леонид Сергеевич* – родился в Саратове (1963), окончил Саратовский государственный университет им. Н.Г. Чернышевского (1985). Защитил диссертацию на соискание ученой степени кандидата физико-математических наук (1991, СГУ) в области радиофизики и нелинейной динамики. Доцент кафедры общей физики СГУ. Опубликовал 50 научных статей.

410012 Саратов ул. Астраханская, 83
Саратовский государственный универсистет им. Н.Г. Чернышевского
E-mail: slskit@mail.ru



*Харин Валерий Николаевич* – родился в 1940 году, окончил физический факультет Воронежского государственного университета (1962). Работал старшим инженером в НИИ физики ВГУ, ведущим инженером, начальником лаборатории, начальником отдела в ЦКБ НПО «Электроника». Впоследствии руководил отделением разработки программного обеспечения САПР в ОКБ при заводе «Процессор», являлся главным конструктором ряда направлений в Министерстве электронной промышленности СССР. В настоящее время работает профессором кафедры ВТиИС, д.т.н., профессор, лауреат Государственной премии СССР и Премии Совета Министров СССР. Имеет более 300 печатных работ, среди которых более 20 монографий и учебных пособий.

394613 Воронежская область, Воронеж, ул. Тимирязева, д. 8
Федеральное образовательное учреждение Воронежская государственная лесотехническая академия
E-mail: Valery-Harin@intercon.ru