

© Василенко В.В.
Vasilenko V.

ОСОБЕННОСТИ СОЗДАНИЯ МИКРОЭЛЕКТРОННОГО УСТРОЙСТВА ГЕНЕРАЦИИ СЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ИМПУЛЬСОВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕХНИЧЕСКИХ СРЕДСТВАХ

FEATURES OF A MICROELECTRONIC DEVICE GENERATE A RANDOM SEQUENCE OF PULSES TO PROTECT THE INFORMATION IN THE TECHNICAL MEANS

Аннотация. Рассмотрены теоретико-прикладные аспекты создания микроселектронного устройства генерации случайной последовательности импульсов для защиты информации в технических средствах. Проанализированы факторы, влияющие на реализуемость устройства. Предложены методические положения оценивания основных параметров устройства и способы компенсации влияния зависимости функционирования его элементов на статистические характеристики случайной последовательности импульсов. Статья подготовлена при финансовой поддержке Министерства образования и науки РФ в рамках федеральной целевой программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007-2013 годы».

Annotation. The theoretical and applied aspects of microelectronic devices generate a random sequence of pulses for the protection of information technology tools. The factors affecting the marketability of the device. The methodical evaluation of the basic parameters of the device and how to compensate for the influence of the functioning of its elements depending on the statistical characteristics of a random sequence of pulses. This article was prepared with financial support from the Ministry of Education and Science under the Federal Target Program "Research and development on priority directions of scientific-technological complex of Russia for 2007-2013".

Ключевые слова. Генератор, параметр, импульс, проводимость, инвертор, кольцо, частота, период, джиттер, случайная величина, закон распределения, энтропия, вероятность, среднееквадратическое отклонение.

Key words. Generator, the parameter, the pulse, the conductivity of the inverter, the ring, the frequency, period jitter, random variable, the distribution of the entropy, probability, standard deviation.

При решении проблем обеспечения безопасности в современных информационно-телекоммуникационных системах широко применяются различные устройства для генерации псевдослучайных и случайных чисел. Такие устройства могут реализовываться на основе генераторов случайной последовательности импульсов и сдвиговых регистров.

Одним из подходов к созданию генератора случайной последовательности импульсов (далее генератора) является использование R независимо функционирующих закольцованных цепочек нечётного числа инверторов (далее колец), выход которых объединён через логическое устройство, реализующее функцию «исключающее или» (далее устройство XOR) [1,2]. Пример схемы рассматриваемого генератора приведен на рис. 1.

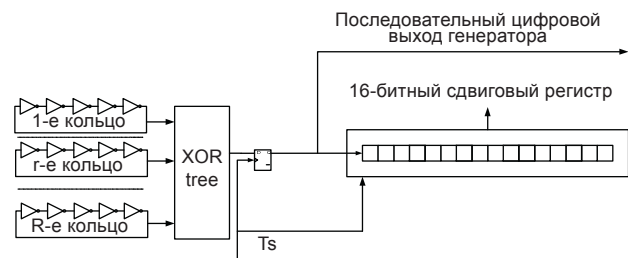


Рис. 1. Схема устройства генератора последовательности случайных импульсов и чисел

В идеальных условиях выходной сигнал

$$\Psi_r(t) = \Psi_r(t + T_r)$$

каждого $г$ -го кольца ($г \in R$) является меандром со сменой выходного состояния (с логического нуля на логическую единицу или обратно) через время T_r , определяемое количеством инверторов N в одном кольце и временем за-

держки смены состояния каждого n-го инвертора τ_{r_n}

$$T_r = \sum_{n=1}^N \tau_{r_n}, r \in R. \quad (1)$$

В реальных условиях время задержки смены состояния каждого инвертора $\tau_{r_n}, r \in R, n \in N$ является случайной величиной, характеризующейся законом распределения, например, плотностью вероятности $f_{r_n}(\tau_{r_n})$ с соответствующим математическим ожиданием $\overline{\tau_{r_n}}$ и среднеквадратическим отклонением $\sigma_{\tau_{r_n}}$ [3].

Очевидно, что при объединении нескольких инверторов в кольцо, период смены состояния r-го кольца T_r также будет случайной величиной (как сумма случайных величин) с законом распределения $f_r(T_r)$, математическим ожиданием

$$\overline{T_r} = \sum_{n=1}^N \overline{\tau_{r_n}}, r \in R \quad (2)$$

и среднеквадратическим отклонением

$$\sigma_r = \sqrt{\sum_{n=1}^N \sigma_{\tau_{r_n}}^2 + 2 \sum_{n < m} K_{nm}}, r \in R, \quad (3)$$

где K_{nm} – корреляционный момент величин τ_{r_n}, τ_{r_m} , знак $n < m$ под суммой обозначает, что суммирование распространяется на все возможные попарные сочетания случайных величин $(\tau_{r_1}, \tau_{r_2}, \dots, \tau_{r_N})$ [3].

При независимости $(\tau_{r_1}, \tau_{r_2}, \dots, \tau_{r_N})$ – случайных величин среднеквадратическое отклонение периода смены состояния r-го кольца определяется по формуле [3]

$$\sigma_r = \sqrt{\sum_{n=1}^N \sigma_{\tau_{r_n}}^2}, r \in R, \quad (4)$$

а при равенстве $\overline{\tau_{r_n}}$ для всех $n \in N$ – по формуле

$$\sigma_r = \sigma_{\tau_{r_n}} \sqrt{N}, r \in R. \quad (5)$$

Закон распределения периода смены состояния r-го кольца $f_r(T_r)$ и, в частности, его среднеквадратическое отклонение σ_r характеризуют так называемый дифференциальный джиттер кольца. Под дифференциальным джиттером кольца будем понимать «отклонение момента смены состояния кольца от его математического ожидания при отсчете времени относительно предыдущей смены состояния кольца». Джиттер по определению является центрированной случайной величиной, распределенной по закону $f_r(T_r - \overline{T_r})$.

Если измерять состояние r-го кольца с периодом T_s S-кратным значению $\overline{T_r}$, то следует рассматривать суммарный джиттер кольца, который также характеризуется соответствующим законом распределения $f_{r_s}(T_s - \overline{T_s})$ со среднеквадратическим отклонением суммы S случайных величин $(T_{r_1}, T_{r_2}, \dots, T_{r_S})$. Под суммарным джиттером кольца будем понимать «отклонение момента S-й смены состояния кольца от его математического ожидания при отсчете времени относительно начала каждого периода T_s ». При этом математическое ожидание момента S-й смены состояния r-го кольца равно

$$\overline{T_{r_s}} = S \cdot \overline{T_r}. \quad (6)$$

Если характеристики колец можно считать одинаковыми, то

$$\overline{T_s} = \overline{T_{r_s}}.$$

В общем случае среднеквадратическое отклонение суммарного джиттера r-го кольца определяется по формуле

$$\sigma_{r_s} = \sqrt{\sum_{n=1}^{S \cdot N} \sigma_{\tau_{r_n}}^2 + 2 \sum_{n < m} K_{nm}}, r \in R, \quad (7)$$

в которой следует учитывать цикличность работы кольца через условие $\sigma_{\tau_{r_n}} = \sigma_{\tau_{r_{n+N}}}$.

При независимости $(\tau_{r_1}, \tau_{r_2}, \dots, \tau_{r_N})$ – случайных величин среднеквадратическое отклонение суммарного джиттера r-го кольца определяется по формуле

$$\sigma_{r_s} = \sigma_r \sqrt{S}, r \in R. \quad (8)$$

На рис. 2 представлена иллюстрация соотношения во времени выходного сигнала кольца и законов распределения дифференциального и суммарного (для периода T_s) джиттеров.

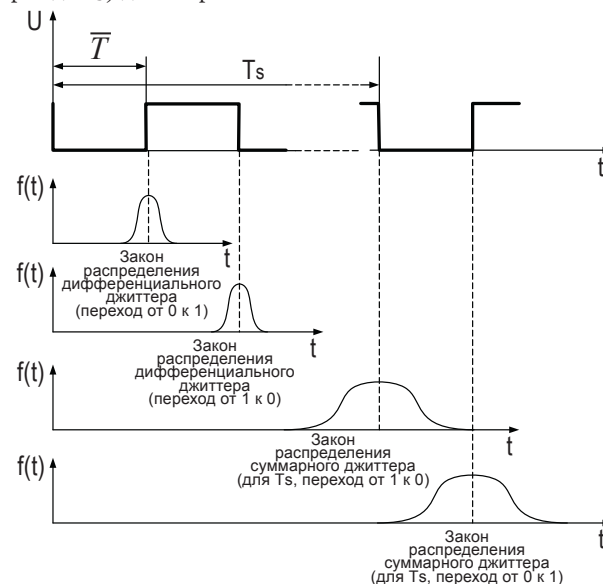


Рис. 2. Иллюстрация соотношений во времени выходного сигнала кольца, законов распределения дифференциального и суммарного джиттеров

В дальнейшем изложении приняты допущения о независимости функционирования инверторов в каждом кольце, независимости функционирования всех колец и нормальном (Гауссовом) виде законов распределения всех джиттеров.

При идеальной синхронизации моментов снятия информации о состоянии кольца с медианой суммарного джиттера теоретически можно получить случайную последовательность импульсов с равновероятной сменой логического нуля и единицы. Однако обеспечение таких условий является весьма сложной технической проблемой.

В качестве иллюстрации рассматриваемых процессов на рис. 3 представлена плотность вероятности суммарного джиттера кольца. Информация о состоянии кольца фиксируется со сдвигом времени t_c относительно медианы суммарного джиттера.

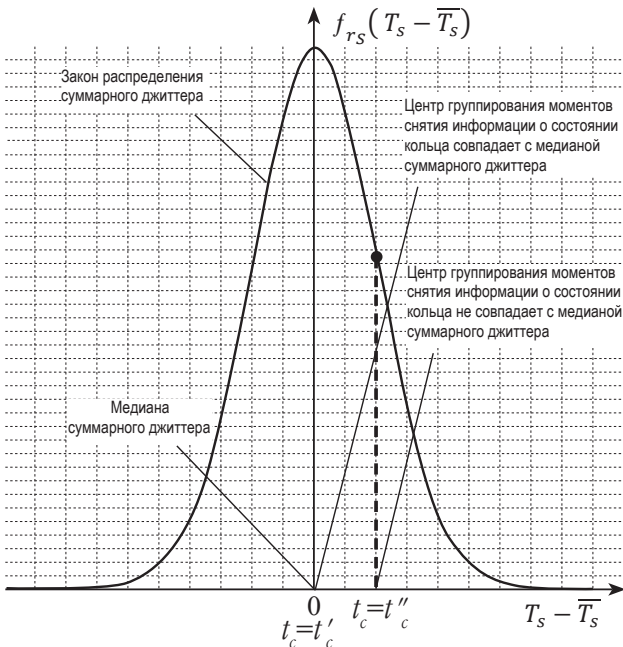


Рис. 3. Иллюстрация закона распределения суммарного джиттера кольца и смещения относительно него центров группирования моментов снятия информации о состоянии кольца

Вероятность смены состояния кольца к моменту t_c вычисляется по зависимости

$$P_{c_{m_r}} = \int_{-\bar{T}_s}^{t_c} f_{r_s}(T_s - \bar{T}_s) d(T_s - \bar{T}_s). \quad (9)$$

В условиях $t_c = t'_c = 0$ (см. рис. 3) вероятность смены состояния кольца при каждом опросе с периодичностью \bar{T}_s будет равна 0,5. Соответственно энтропия кольца на один бит, вычисляемая по зависимости

$$H_r = -P_{c_{m_r}} \cdot \log_2 P_{c_{m_r}} - (1 - P_{c_{m_r}}) \log_2 (1 - P_{c_{m_r}}), \quad (10)$$

будет иметь максимальное значение, равное 1.

При смещении моментов снятия информации с выхода кольца относительно медианы суммарного джиттера значение энтропии снижается. На рисунке 3 это соответствует условию $t_c = t''_c$. Вероятность смены состояния кольца к моменту t''_c будет больше 0,5. В общем случае, при несовпадении моментов снятия информации о состоянии кольца с медианой суммарного джиттера всегда будет выполняться условие $P_{c_{m_r}} \neq 0,5$, и, как следует из выражения (10), значение энтропии кольца на один бит будет меньше единицы.

Зависимость энтропии кольца на один бит от рассматриваемого смещения применительно к нормальному закону распределения суммарного джиттера пред-

ставлена на рис. 4 (смещение оценивается в долях среднеквадратического отклонения суммарного джиттера).

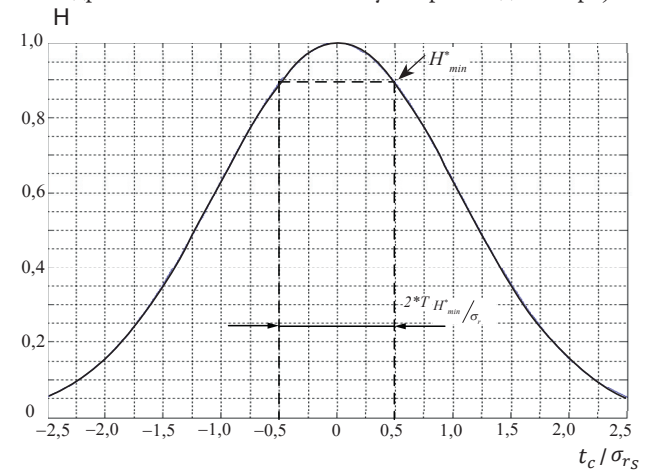


Рис.4. Зависимость энтропии кольца на один бит от смещения момента снятия информации о состоянии кольца относительно медианы суммарного джиттера

Важно отметить, что момент снятия информации с выхода кольца также представляет собой случайную величину, распределенную на конечном интервале времени по определённому закону с дисперсией, в лучшем случае меньшей дисперсии джиттера кольца. На практике генератор импульсов опроса состояния кольца может представлять собой такое же кольцо или более стабильный генератор импульсов со своим джиттером. При этом значение энтропии, соответствующее предельному отклонению моментов снятия информации о состоянии кольца относительно медианы суммарного джиттера кольца, является оценкой его минимального возможного значения H_{min} . Математическое ожидание энтропии будет принимать промежуточное значение между H_{min} и 1, в зависимости от параметров закона распределения джиттера генератора опроса. На рис.5 в качестве примера влияния рассматриваемого фактора на оценку энтропии, представлена зависимость математического ожидания энтропии кольца на один бит от длительности интервала равномерного распределения джиттера генератора опроса T_{ch} при совпадении его среднего значения с медианой суммарного джиттера кольца. На графике длительность интервала джиттера генератора опроса представлена долей от среднеквадратического отклонения суммарного джиттера кольца. Сравнительный анализ данных, представленных на рис. 4 и 5, подтверждает положение о том, что оценки энтропии с учётом закона распределения джиттера генератора опроса выше минимальных (гарантированных) оценок.

С момента начала независимого функционирования колец и генератора импульсов опроса суммарные джиттеры каждого из них в измерении относительно об-

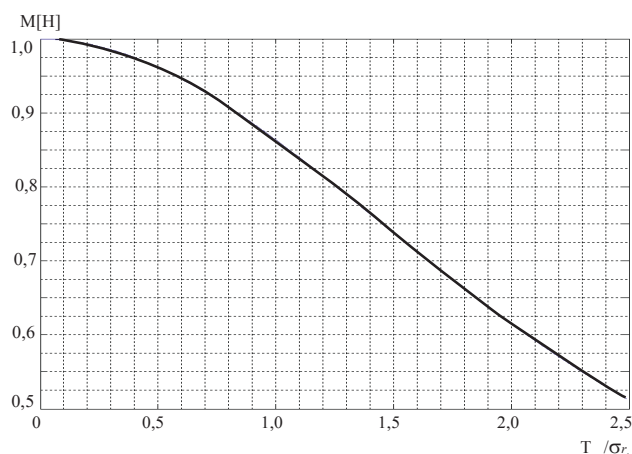


Рис.5. Зависимость математического ожидания энтропии кольца на один бит от длительности интервала джиттера генератора опроса при его равномерном распределении и совпадении среднего значения с медианой суммарного джиттера

щего старта будут нарастать. Среднеквадратические отклонения этих джиттеров могут быть вычислены по формулам (7), (8) при рассмотрении параметра S в качестве порядкового номера цикла смены состояния кольца от момента начала их функционирования. Очевидно, что существует такое количество циклов смены состояния колец S_n , после которого среднеквадратическое отклонение суммарного джиттера любого кольца $\sigma_{r_{S_n}}$ станет намного больше периода опроса его состояния \bar{T}_s . Это означает, что после S_n циклов функционирования колец центры группирования (медианы) джиттеров колец и генератора опроса будут практически равновероятно и независимо распределены на интервале \bar{T}_s . Если задаться допустимым минимальным значением энтропии кольца на один бит H_{min}^* , то на основании закона распределения суммарного джиттера кольца $f_{r_s}(T_s - \bar{T}_s)$ можно вычислить и поставить ему в соответствие допустимый интервал смещения момента снятия информации о состоянии кольца относительно медианы суммарного джиттера $T_{H_{min}^*}$ (рис. 4). В этом случае вероятность реализации заданной минимальной энтропии кольца на один бит $P_{r_s}^{H_{min}^*}$ для одного кольца может быть выражена через вероятность попадания импульса опроса состояния кольца в интервал $T_{H_{min}^*}$, равновероятно располагаемый на интервале \bar{T}_s

$$P_{r_s}^{H_{min}^*} = \frac{T_{H_{min}^*}}{\bar{T}_s}. \quad (11)$$

При сложившихся в современной микроэлектронике соотношениях параметров дифференциальных джиттеров колец и задержек смены их состояния (менее 0,01), значение вероятности реализации заданной минимальной энтропии выходной последовательности генератора, основанного на функционировании одного кольца, принимает недопустимо малые значения.

Указанным обстоятельством и обусловлена необходимость применения совокупности R независимо функционирующих одинаковых колец. При этом реализуемость рассматриваемого подхода связана с асимптотическим приближением закона распределения центров группирования джиттеров колец и генератора опроса на каждом интервале \bar{T}_s к равномерному через ограниченный интервал времени с момента начала работы генератора, а также отсутствием абсолютной статистической зависимости между кольцами (что будет показано ниже).

Важным вопросом является принцип объединения выходов R независимо функционирующих колец. Этот принцип заключается в необходимости обеспечения при каждом опросе состояния колец значения итоговой энтропии не меньше максимального среди энтропий отдельных колец. Такому принципу полностью удовлетворяет логическая функция «исключающее или» (XOR). Она всегда обеспечивает выходную энтропию не меньше, чем значение максимальной энтропии среди всех независимых входных сигналов. В предельном случае при наличии только одного входа с ненулевой энтропией и нулевой энтропией всех остальных входов – выходная энтропия функции XOR будет равна энтропии этого единственного входа.

Объединение всех колец через устройство XOR позволяет определить надежность реализации заданной минимально допустимой энтропии на один бит разрабатываемого генератора случайной последовательности импульсов $P_S^{H_{min}^*}$ через вероятность попадания импульса генератора опроса при каждом снятии информации в интервал $T_{H_{min}^*}$ хотя бы одного кольца. Значение такой вероятности вычисляется по формуле

$$P_S^{H_{min}^*} = 1 - (1 - P_{r_s}^{H_{min}^*})^R. \quad (12)$$

При этом с вероятностью $(1 - P_S^{H_{min}^*})$ возможно появление выходного импульса генератора с энтропией, меньше заданной.

На основании рассматриваемой теоретико-вероятностной модели, задаваясь требуемыми значениями H_{min}^* и $P_S^{H_{min}^*}$, представляется возможным определять необходимое количество колец R^* в генераторе по формуле

$$R^* = \frac{\ln(1 - P_S^{H_{min}^*})}{\ln(1 - P_{r_s}^{H_{min}^*})}. \quad (13)$$

Иллюстративные примеры требуемого количества колец R^* в генераторе для различных вариантов отношения среднеквадратического отклонения суммарного джиттера кольца σ_{r_s} к периоду опроса его состояния \bar{T}_s , а также требуемых значений H_{min}^* и $P_S^{H_{min}^*}$ представлены в таблице.

Иллюстративные примеры требуемого количества колец R^* в генераторе

R^*	$H_{min}^* = 0,9$			$H_{min}^* = 0,95$			$H_{min}^* = 0,99$		
	$P_S^{H_{min}^*} = 0,9$	$P_S^{H_{min}^*} = 0,95$	$P_S^{H_{min}^*} = 0,99$	$P_S^{H_{min}^*} = 0,9$	$P_S^{H_{min}^*} = 0,95$	$P_S^{H_{min}^*} = 0,99$	$P_S^{H_{min}^*} = 0,9$	$P_S^{H_{min}^*} = 0,95$	$P_S^{H_{min}^*} = 0,99$
$\sigma_{r_s}/\bar{T}_s = 0,01$	240	312	479	343	446	686	777	1011	1554
$\sigma_{r_s}/\bar{T}_s = 0,005$	480	624	960	687	893	1373	1555	2023	3110
$\sigma_{r_s}/\bar{T}_s = 0,001$	2403	3126	4805	3436	4470	6872	7778	10120	15556

Для современного уровня развития микроэлектроники представленные в таблице оценки требуемого количества колец в генераторе являются вполне достижимыми.

Теперь проанализируем возможности достижения задаваемых характеристик генератора при снятии принятых ранее допущений, касающихся нормальности закона распределения джиттеров, независимости функционирования инверторов в каждом кольце, независимости функционирования всех колец.

Известны работы, посвященные исследованию природы и характеристик рассматриваемых джиттеров, в которых экспериментально подтверждается нормальный вид законов их распределения [4,5]. Несмотря на это, допущение о нормальности законов распределения джиттеров может быть снято, поскольку их вид не оказывает влияния на функционирование рассматриваемого генератора. Закон распределения нужен только при проектировании устройства для оценки интервала $T_{H_{min}^*}$ (рис. 4). Предположение о нормальном виде закона распределения всего лишь облегчает процедуру экспериментальной оценки его параметров и позволяет проводить аналитические вычисления вместо применения численных методов.

Для анализа статистической зависимости функционирования инверторов и колец воспользуемся приближенной формулой оценки времени переключения схемы типового инвертора, реализованного на компланарной (дополняющей) паре полевых транзисторов [6]

$$\tau_{rn} \approx \frac{1,6 \cdot C_n}{b \cdot E_n}, \quad (13)$$

где b – удельная проводимость полевого транзистора (одинакова для обоих транзисторов);

E_n – напряжение источника электропитания устройства;

C_n – ёмкость нагрузки инвертора (ёмкость входа следующего инвертора).

Анализ выражения (13) показывает, что у каждого инвертора существует независимый стохастический источник джиттера, которым является естественная шумовая составляющая удельной проводимости полевого транзистора. Следовательно, абсолютная статистическая зависимость в функционировании инверторов, джиттеров колец и генератора импульсов опроса отсутствует, а коэффициенты их взаимной корреляции по модулю всегда будут меньше единицы. При этом уровень шумовой составляющей удельной проводимости полевых транзисторов пропорционально зависит от температуры окружающей среды, что в соответствии с принципом получения гарантированного результата обуславливает необходимость оценивания джиттеров на этапе проектирования в условиях минимальной температуры заданного в технических условиях диапазона.

В то же время из анализа выражения (13) следует, что в принципе возможна некоторая зависимость пар инверторов через ёмкость нагрузки.

Очевидна также определённая зависимость функционирования инверторов, колец и генератора импульсов опроса по питанию устройства. При этом изменения напряжения электропитания действуют на инверторы, кольца и генератор импульсов опроса одновременно и с одинаковыми последствиями: при уменьшении напряжения питания все джиттеры увеличиваются, а при увеличении напряжения питания все джиттеры уменьшаются.

В этой связи для учета и компенсации влияния корреляционных связей между элементами генератора на качество его функционирования возможны следующие подходы:

- после исследования стабильности источника электропитания генератора, расчеты и измерения законов распределения дифференциального и суммарного джиттеров кольца $f_r(T_r - \bar{T}_r)$, $f_{r_s}(T_s - \bar{T}_s)$ необходимо

проводить при максимально реализуемом напряжении источника электропитания. Это соответствует принципу гарантированной оценки минимальной энтропии (в связи с уменьшением значения интервала $T_{H_{min}^*}$ и, как следствие, приводит к увеличению потребного количества колец;

- после экспериментальной оценки автокорреляционной функции кольца по циклам смены его состояния и последующего вычисления длительности автокорреляционного интервала $S_{ки}$ (измеренного в количестве циклов смены состояния кольца) период опроса состояния колец \overline{T}_s необходимо задавать исходя из условия $S > S_{ки}$;

- если последнее условие приводит к снижению выходной частоты генератора ниже требуемой F_S^{mp} , то необходимо проводить экспериментальные оценки условий следует рассматривать возможные комбинации предшествующих состояний кольца) и для проектных решений принимать условную вероятность джиттера с минимальным значением среднеквадратического отклонения. Это также соответствует принципу гарантированной оценки минимальной энтропии и связано с дополнительным увеличением потребного количества колец.

Эффективным направлением повышения качества генератора случайной последовательности импульсов в части энтропии на один бит и надёжности её обеспечения является использование эластичной функции на выходе генератора [1,2]. Платой за дополнительное качество генератора при этом будет снижение скорости выходного потока импульсов.

Таким образом, основными параметрами рассматриваемого генератора являются:

N – количество инверторов, из которых состоит одно кольцо;

R – количество независимых колец;

S – количество циклов смены состояния кольца, входящих в один цикл опроса его состояния;

\overline{T}_s – математическое ожидание периода следования выходных импульсов (логических нулей и единиц) генератора (частота следования выходных импульсов генератора $F_s = 1/\overline{T}_s$);

S_n – количество циклов смены состояния колец (отсчитываемое от начала работы генератора), после которого центры группирования джиттеров колец и генератора опроса будут практически равновероятно распределены на интервале \overline{T}_s ;

$S_{ки}$ – длительность автокорреляционного интервала кольца;

$\overline{\tau}_{rn}$ – математическое ожидание задержки смены

состояния инвертора;

$\sigma_{\tau_{rn}}$ – среднеквадратическое отклонение задержки смены состояния инвертора;

$f_r(T_r - \overline{T}_r)$ – плотность вероятности дифференциального джиттера кольца;

\overline{T}_r – математическое ожидание периода смены состояния кольца;

σ_{r_s} – среднеквадратическое отклонение джиттера кольца;

$f_{r_s}(T_s - \overline{T}_s)$ – плотность вероятности суммарного джиттера кольца;

σ_{r_s} – среднеквадратическое отклонение суммарного джиттера кольца;

H_{min} – минимальное значение энтропии генератора на один бит;

$P_S^{H_{min}}$ – надёжность реализации минимальной энтропии на один бит генератора.

Параметры F_s , S_n , $S_{ки}$, $\overline{\tau}_{rn}$, $\sigma_{\tau_{rn}}$, \overline{T}_r , σ_r , σ_{r_s} , H_{min} , $P_S^{H_{min}}$ и плотности вероятностей $f_r(T_r - \overline{T}_r)$, $f_{r_s}(T_s - \overline{T}_s)$ при разработке генератора оцениваются расчётными (в том числе с использованием приведенных в статье зависимостей) и инструментальными методами [7]. При этом в схемотехнических решениях следует ориентироваться на конструктивное увеличение дифференциального джиттера колец.

Требования к основным выходным функциональным свойствам генератора задаются через допустимое минимальное значение энтропии генератора на один бит H_{min}^* , требуемую надёжность реализации заданной минимально допустимой энтропии $P_S^{H_{min}^*}$ и требуемую частоту следования выходных импульсов генератора F_S^{mp} .

Оптимизируемыми параметрами являются R, N и S.

Выбор оптимальных значений R^* , N^* , S^* может проводиться с использованием известных методов направленного перебора [8].

Выводы.

1. Основой существования энтропии генерируемой импульсной последовательности является наличие независимых стохастических источников джиттера у всех колец, которыми являются естественные шумовые составляющие удельных проводимостей каждого из используемых полевых транзисторов;

2. Генератор случайных чисел с высокими статистическими характеристиками может быть реализован на основе приемлемого для современного уровня развития микроэлектроники количества независимо функционирующих колец инверторов. При этом к инверторам могут не предъявляться высокие требования по показа-

телям стабильности динамических характеристик;

3. Предложены соответствующие принципу гарантированного конечного результата методические положения оценивания основных параметров генератора

на этапе проектирования, а также способы компенсации влияния взаимной зависимости функционирования его элементов на статистические характеристики случайной последовательности импульсов.

Литература.

1. Sunar B., Martin WJ., Stinson D.R. *A Provably Secure True Random Number Generator with Built-in Tolerance to Active Attacks*. *IEEE Transactions on Computers*, vol 58, no 1, pages 109-119, January 2007.
2. Chengxin Liu. *Jitter in Oscillators with $1/f$ Noise Sources and Application to True RNG for Cryptography*. A Dissertation submitted to the Faculty of the WORCESTER POLYTECHNIC INSTITUTE.
3. Феллер В. *Введение в теорию вероятностей и её приложения*, тт. 1-2 – М.: Мир, 1984.
4. Ali Hajimiri, Sotirios Limotyrakis, Thomas H. Lee. *Jitter and Phase Noise in Ring Oscillators*. *IEEE JOURNAL OF SOLID-STATE CIRCUITS*, VOL. 34, NO. 6, JUNE 1999.
5. John A. McNeill. *Jitter in Ring Oscillators*. *IEEE JOURNAL OF SOLID-STATE CIRCUITS*, VOL. 32, NO. 6, JUNE 1997.
6. Довгун В.П. *Электротехника и электроника. Курс лекций. Лекция 28.-Институт космических и информационных технологий СФУ, 2008-2010.*
7. Ракк М.А. *Измерения в цифровых системах передачи*. – М.: Маршрут, 196 стр., 2004.
8. Михалевич В.С., Трубин В.А., Шор Н.З. *Оптимизационные задачи производственно-транспортного планирования*. – М.: Наука, 264 стр., 1986.

Материал поступил в редакцию 02. 08. 2012 г.