Технические науки

УДК 004.04

Коряков Игорь Витальевич

Начальник отдела разработки и производства технических средств

ООО Научно-внедренческая фирма «Криптон»

ХОРОШИЙ ИСТОЧНИК ЭНТРОПИИ

Аннотация: *В данной работе рассматриваются вопросы создания источника энтропии для применения в генераторах случайных бит для криптографических приложений. Показано, что характеристики источника энтропии можно приблизить к идеальным настолько, что для обнаружения отличия такого источника от идеального потребуется очень много времени.*

Ключевые слова: *энтропия, криптография, генератор случайных бит, тепловой шум.*

Введение

При построении недетерминированного (физического, истинного) генератора случайных бит (чисел, последовательностей) для криптографических приложений требуется хороший источник энтропии, причём традиционно принято считать, что такие физические источники всегда плохи по своим статистическим параметрам и эти параметры требуется улучшать дополнительным оборудованием и алгоритмами для «выравнивания статистических характеристик».

Мы же попробуем построить источник энтропии с характеристиками, настолько близкими к идеальным, что для обнаружения отличия такого источника от идеального потребуется очень много времени, то есть длина анализируемой последовательности будет нереально большой.

Хороший генератор шума

Основой хорошего источника энтропии может быть только некий фундаментальный физический процесс, то есть, незыблемое явление природы, а не какое-нибудь технологическое достижение. Например, напряжение теплового шума на концах проводника (резистора) порождается фундаментальным явлением природы, а шумовое напряжение, определяемое эффектом лавинного пробоя обратно смещённого p-n перехода, является технологическим достижением.

Рассмотрим генератор шума на основе теплового шума.

Не забываем, что напряжение теплового шума создаётся активной составляющей комплексного сопротивления любой цепи, независимо от того, сколько там резисторов и есть ли они вообще [1, с.112]. ЭДС теплового шума e_t равна (в современной нотации)

$$e_t = \sqrt{4kTRB},$$

где k – постоянная Больцмана (1.38e–23), T – температура в град. Кельвина, R – активная составляющая сопротивления цепи в Омах и B – ширина полосы шума в Гц.

Обычно генератор на основе теплового шума содержит резистор и усилитель. Эквивалентная схема такого генератора приведена на рисунке 1.

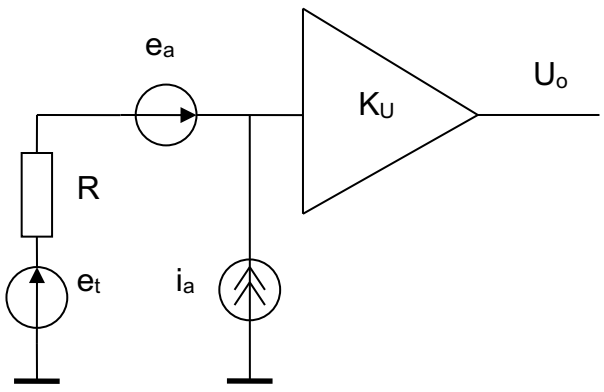


Рисунок 1 – Эквивалентная схема генератора шума

Здесь R – активная составляющая сопротивления цепи, генерирующая ЭДС e_t, e_a – источник напряжения собственного шума усилителя, i_a – источник тока собственного шума усилителя, K_U – коэффициент усиления усилителя по напряжению (считаем входное сопротивление усилителя бесконечным), U_o – выходное напряжение усилителя.

Чтобы шум на выходе был максимально «чистый», нам требуется минимизировать коэффициент шума NF, определяющий вклад собственных шумов усилителя в выходной сигнал:

$$NF = 1 + \frac{P_a}{P_t},$$

где P_a – мощность собственных шумов усилителя, P_t – мощность теплового шума, генерируемого активной составляющей сопротивления входной цепи.

Считая полосы всех шумов и коэффициент усиления для всех шумов одинаковыми, можем выразить NF через параметры источников шума:

$$NF = 1 + \frac{\frac{e_a^2}{R} + i_a^2 R}{4kT}.$$

И, если мы при заданных e_a и i_a выбрали значение R, минимизирующее NF, то зная необходимое значение U_o, мы сможем рассчитать требуемый коэффициент усиления K_U.

Рассмотрим численный пример: усилитель с e_a = 1.1 нВ/Гц$^{1/2}$ и i_a = 8.8 пА/Гц$^{1/2}$. И мы берём R побольше, чтобы шума было побольше. Подставляем в формулу 10 кОм и получаем NF = 49.4. Многовато. Чтобы внутренние шумы были хотя бы не больше полезного шума, нужно, чтобы NF = 2. Методом итераций получаем R = 120 Ом и NF = 2.2.

Это неплохой результат, тем более, что внутри усилителя тоже есть источники теплового шума, которые не испортят исходного хорошего шу-

ма резистора.

Если требуется получить эффективное значение U_o = 100 мВ (для нормально распределённого шума это порядка 0.8 В пик-пик), то при T = 290 K° и полосе 500 МГц получим:

$$K_U = \frac{U_o}{\sqrt{4kTRB}} = \frac{0.1}{\sqrt{4 \cdot 1.38e-23 \cdot 290 \cdot 120 \cdot 500000000}} = \frac{0.1}{30.98e-6} = 3227\cdot$$

Далее для получения источника энтропии необходимо превратить аналоговый шумовой сигнал в цифровой. Эту операцию выполняет АЦП. Почему АЦП, а не, например, компаратор? Потому, что идеальный АЦП при идеальном случайном сигнале порождает независимые случайные значения на своих двоичных выходах. Энтропия этих отдельных бит в реальном АЦП с реальным шумом на входе может быть недостаточно высока, но использование многих разрядов АЦП позволяет получить выходную последовательность случайных бит, близких к идеалу.

Нарушение теоремы отсчётов

При частоте дискретизации F_s теорема отсчётов справедлива не только для сигналов, спектр которых ограничен частотами от 0 до F_s / 2, но и для сигналов в полосах от F_s / 2, до F_s, от F_s до 3F_s / 2, и так далее. Эти полосы называются зонами Найквиста: 1-я зона, 2-я зона, 3-я.

Современные АЦП технологически подтягиваются к этой возможности и позволяют работать не только в 1-й зоне, но и в гораздо более высоких по номерам зонах. Например, нам необходимо обрабатывать сигнал с шириной полосы 30 МГц, в диапазоне частот от 450 до 480 МГц. Для этого нам необходимо поставить на входе АЦП полосовой фильтр, выделяющий требуемый диапазон частот 450 – 480 МГц, и работать при частоте дискретизации 60 МГц в 16-той зоне Найквиста так, как будто этот диапазон лежит в области от 0 до 30 МГц. Необходимо только помнить, что для нечётных зон Найквиста спектр сигнала остаётся неизменным, а для чётных –

зеркально разворачивается, то есть при изменении частоты исходного сигнала от нижней границы к верхней границе зоны, частота результирующего сигнала, представленного в первой зоне, будет изменяться от верхней границы к нижней. При этом сохраняется однозначное соответствие между аналоговым сигналом как непрерывной функцией и сигналом, представленным цифровыми отсчётами (с точностью до зоны Найквиста).

А теперь нарушим теорему отсчётов. Возьмём сигнал с полосой от 0 до 480 МГц и оцифруем его без всяких фильтров с частотой F_s = 60 МГц. Мы получим отсчёты суммы сигналов в 16-ти зонах Найквиста, причём составляющие суммы из чётных зон будут зеркально повёрнуты. Это явление называется эффектом наложения и считается вредным.

Мощность результирующего сигнала станет равной суммарной мощности составляющих всех зон Найквиста, а однозначное соответствие между аналоговым сигналом и значениями отсчётов будет необратимо утеряно.

На рисунках 2 и 3 показаны графики непрерывного шумового сигнала с полосой 30 МГц и сигнала с полосой 480 МГц соответственно (жирными точками показаны отсчёты с частотой дискретизации 60 МГц).

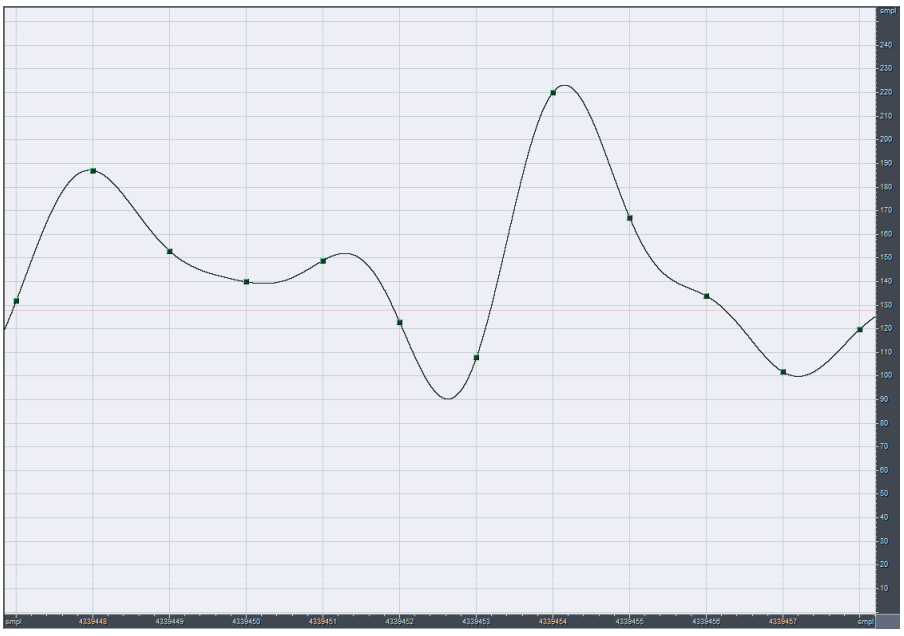


Рисунок 2 – Шумовой сигнал с полосой 30 МГц

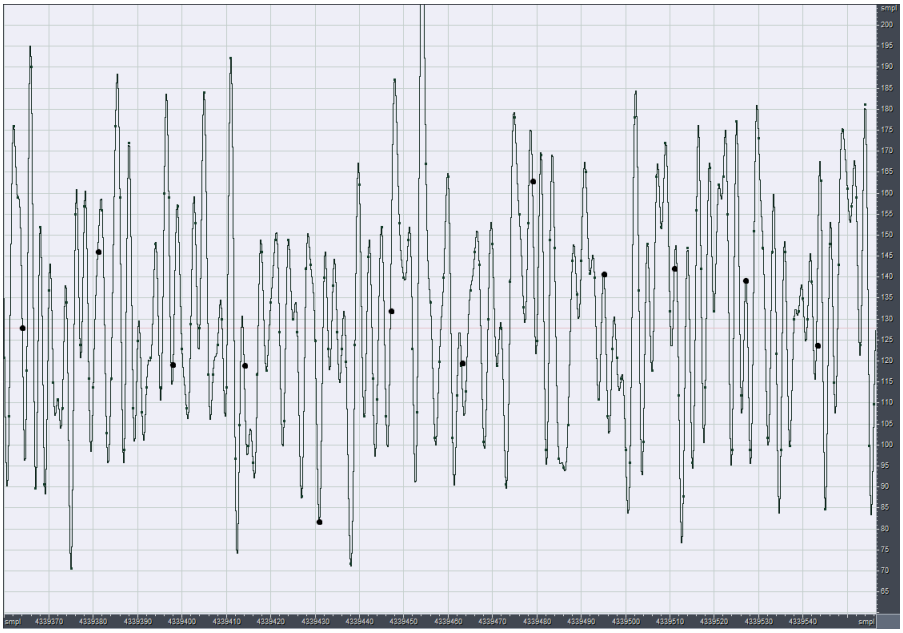


Рисунок 3 – Шумовой сигнал с полосой 480 МГц

Дискретизация широкополосного шума

Если мы возьмём широкополосный сигнал от физического источника шума и подвергнем его аналого-цифровому преобразованию с частотой дискретизации, существенно меньшей верхней частоты шумового сигнала, то мы получим эффект наложения.

Что он даёт:

1. Всё нормализуется, то есть суммирование множества независимых случайных величин, даже не совсем нормальных, приводит к нормальному распределению плотности вероятности суммарного сигнала.

2. Не совсем белый шум обеляется в степени усреднения.

3. Возрастает мощность шума в n раз по сравнению с применением узкополосного аналогового фильтра в 1-й зоне Найквиста.

4. Корреляция между отсчётами исходного сигнала уменьшается в степень раз.

То есть, сигнал, возможно неидеальный, идеализируется в степени,

соответствующей числу усреднений. Практически, 16 – это более, чем достаточно.

Исчезающее различие

Пусть имеются две независимые двоичные последовательности a и b с вероятностями нуля и единицы соответственно p_0, p_1 и смещением $d = |p_0 - p_1|$. Тогда при суммировании по модулю 2 последовательностей a и b смещение вероятности нуля и единицы для суммарной последовательности будет равно $2d^2$. В общем случае, ожидание смещения суммы m независимых последовательностей с одинаковыми смещениями будет иметь порядок m-ой степени ожидания смещения одной последовательности.

Для доверительной вероятности β и числа элементов последовательности N определим допустимый интервал ε, в который должно попадать смещение d при равенстве $p_0 = p_1$, как

$$\varepsilon = \frac{1}{2\sqrt{N}} \arg\Phi * \left(\frac{1+\beta}{2} \right).$$

Для того, чтобы с вероятностью β смещение d_m суммы m последовательностей длиной N не вышло за пределы допустимого интервала ε, т. е. для выполнения условия $d_m < \varepsilon$, можно определить минимальное требуемое число m суммируемых последовательностей как

$$m = \left\lceil \frac{\ln d}{\ln \varepsilon} \right\rceil.$$

Ниже приведены значения m для ряда значений β, d и N.

N	β	ε	d=30%	d=10%	d=1%	d=0.1%
10^6	0.99	0.00135	m=8	m=4	m=2	m=2
	0.999	0.00165	m=6	m=3	m=2	m=1
	0.9999	0.002	m=5	m=3	m=2	m=1
10^{12}	0.99	0.00000135	m=12	m=6	m=3	m=2
	0.999	0.00000165	m=12	m=6	m=3	m=2
	0.9999	0.000002	m=11	m=6	m=3	m=2

В качестве независимых последовательностей для суммирования могут быть выбраны отдельные разряды АЦП (для исключения возможных корреляционных связей между разрядами мы задержим значения различных разрядов на различное число тактов). Если использовать m-разрядный АЦП, то оценка величины допустимого интервала ε при заданном значении d составит

$$\varepsilon = \exp(m \cdot \ln d).$$

Например, для 8-ми разрядного АЦП при $m = 8$ и $d < 1\%$, получим оценку интервала $\varepsilon = 1e{-}16$.

В соответствии с законом повторного логарифма (предельный закон теории вероятностей) нижеследующее условие может быть нарушено при некотором достаточно большом n, если последовательность отличается от идеальной последовательности Бернули

$$x_n < \sqrt{(2 \ln \ln n)/n}.$$

Здесь x_n – оценка отклонения вероятности значений последовательности от значения ожидания 0.5 на n опытах, равная

$$x_n = \frac{\sum_{k=0}^{n-1}(b_k - 0.5)}{n},$$

где b_k – k-тый бит последовательности.

Наша степень отличия – это значение x_n, сравнимое с границами интервала $\varepsilon = 1e{-}16$, по значению которого мы легко вычисляем $n = 1.0e33$.

Если наш генератор производит случайные биты со скоростью 60 Мбит/с, то время обнаружения отличия нашей последовательности от идеальной последовательности Бернули составит:

1.0e33 / 60000000 / 3600 / 24 / 366 = 5e18 лет.

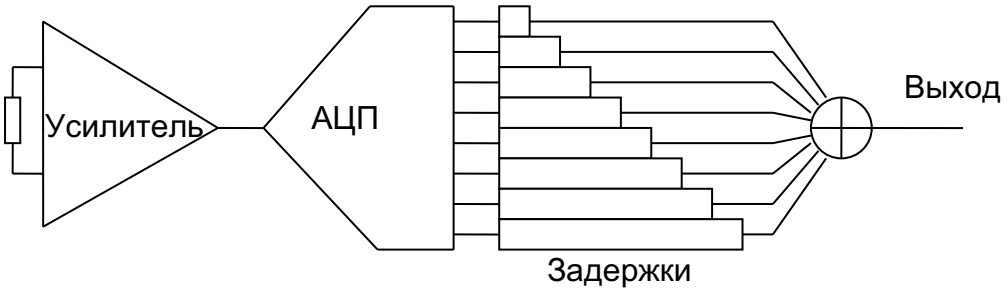
Похоже, мы даже немного перестарались.

Даже для $m = 8$ и $d < 5\%$, получим оценку интервала $\varepsilon = 4e{-}11$, для

которой вычисляем n = 1e22 и 1.0e22 / 60000000 / 3600 / 24 / 366 = 5.2 млн лет.

Выводы

Итак, наш источник энтропии состоит из генератора шума в виде резистора с усилителем и АЦП, часть разрядов которого задерживается на различное число тактов и складывается по модулю 2, образуя выходную последовательность случайных бит. Этого достаточно, никаких дополнительных или иных элементов для источника энтропии не требуется, они будут лишними.



Мы построили скелет источника энтропии с характеристиками, близкими к идеальным. Такой источник может стать основой генератора истинно случайных бит, близкого к идеальному.

Для завершения создания генератора необходимо добавить узлы питания (особо «чистым» должно быть питание генератора шума), цепи контроля узлов питания, узел контроля качества источника шума, узлы, реализующие тесты включения, инициализации, периодические и по запросу оператора, непрерывные тесты первичных последовательностей, тесты выходной случайной последовательности, узлы блокировки работы генератора при нарушении условий его правильного функционирования, контроллер обмена с потребителем (компьютером). Необходимо также реализовать электрические и механические требования по предотвращению внешних электромагнитных наводок и других возможных неблагоприятных воздей-

ствий на генератор.

Кроме того, генератор должен быть оснащён драйверами, библиотекой функций API для создания приложений, тестовым программным обеспечением.

Вот тогда это будет полноценный недетерминированный генератор истинно случайных бит.

Литература

1. Nyquist, H. (1928). "Thermal Agitation of Electric Charge in Conductors". Physical Review. 32 (110): 110–113.

ПРИЛОЖЕНИЕ 1

Схемотехника генератора аналогового шума на основе источников тепловых шумов

Ещё раз напоминаем, что e_t образуется активной составляющая комплексного сопротивления входной цепи усилителя, независимо от её конфигурации (великий Найквист после своей знаменитой формулы сделал приписку: «for any circuit»).

Рассмотрим несколько схем генератора на основе теплового шума (далее R – шумящий резистор, R_f – резистор в цепи обратной связи ОУ, e_t – источник ЭДС теплового шума, U_o – выходное напряжение ОУ). Первая схема приведена на рисунке П1.

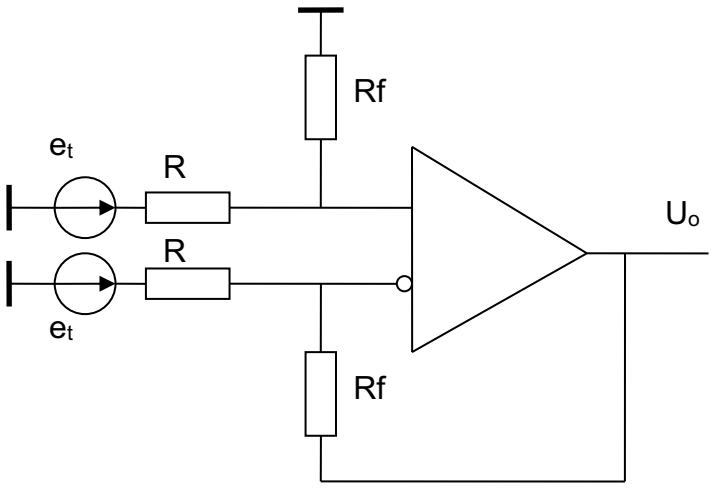


Рисунок П1 – Первая схема генератора.

Для этой схемы считаем сопротивление R_f существенно превышающим сопротивление шумящих резисторов и, поскольку ЭДС шумов резисторов e_t независимы, то

$$U_o = \frac{\sqrt{2} e_t R_f}{R} .$$

При увеличении величины сопротивления резисторов R в два раза получим:

$$U_o = \frac{2\sqrt{2} e_t R_f}{2R} = \frac{\sqrt{2} e_t R_f}{R} ,$$

то есть, U_o остаётся неизменным.

Во второй схеме, приведённой на рисунке П2, выходное напряжение ОУ составит

$$U_o = \frac{e_t R_f}{R} .$$

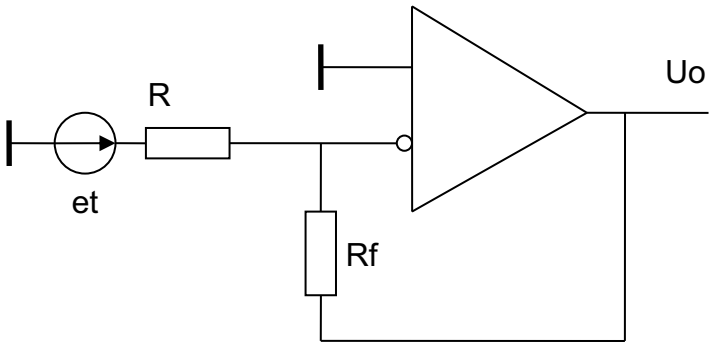


Рисунок П2 – Вторая схема генератора.

При увеличении величины сопротивления резисторов R в два раза получим:

$$U_o = \frac{\sqrt{2} e_t R_f}{2R} ,$$

то есть, U_o уменьшится в корень из 2-х раз.

В третьей схеме, приведённой на рисунке П3, Выходное напряжение

ОУ составит

$$U_o = \frac{e_t R_f}{R_i} .$$

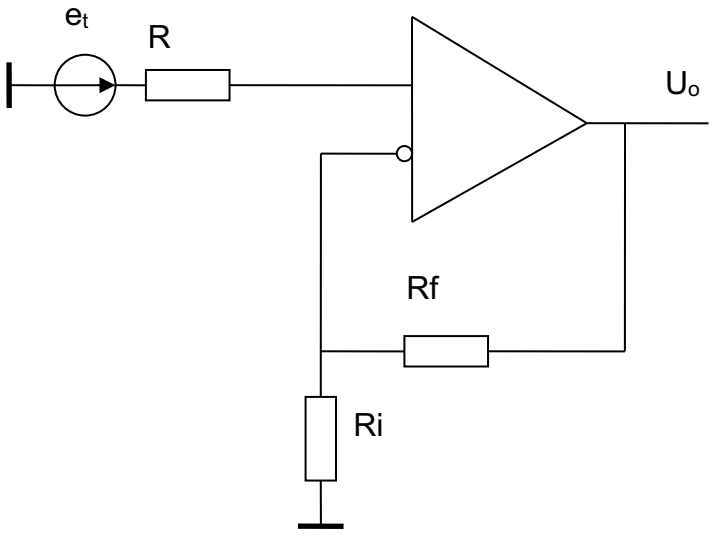


Рисунок П3 – Третья схема генератора.

При увеличении величины сопротивления резистора *R* в два раза получим:

$$U_o = \frac{\sqrt{2} e_t R_f}{R_i} ,$$

то есть, U_o увеличится в корень из 2-х раз.

В четвёртой схеме, приведённой на рисунке П4, выходное напряжение ОУ составит

$$U_o = \frac{\sqrt{2} e_t R_f}{R_i} .$$

При увеличении величины сопротивления резистора *R* в два раза получим:

$$U_o = \frac{2\sqrt{2} e_t R_f}{R_i} ,$$

то есть, U_o увеличится в 2 раза.

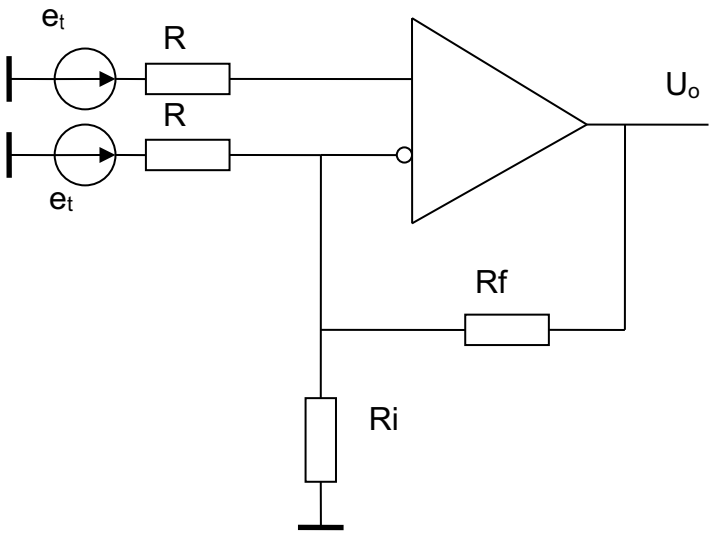


Рисунок П4 – Четвёртая схема генератора.

Рассмотрим ещё раз эквивалентную схему генератора шума с учётов шумов усилителя, приведённую на рисунке П5.

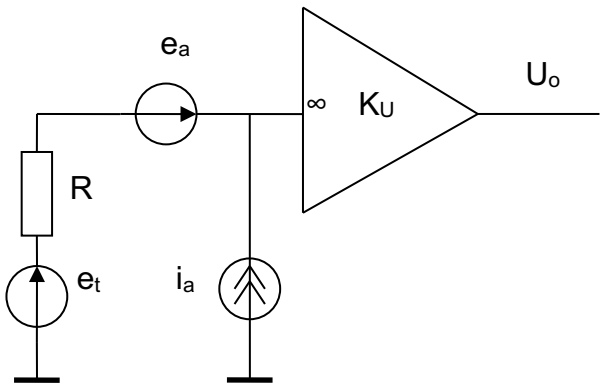


Рисунок П5 – Эквивалентная схема генератора.

Здесь R – активная составляющая сопротивления цепи, генерирующая ЭДС e_t, e_a – источник напряжения собственного шума усилителя, i_a – источник тока собственного шума усилителя, K_U – коэффициент усиления усилителя по напряжению (считаем входное сопротивление усилителя бесконечным), U_o – выходное напряжение усилителя.

Чтобы шум на выходе был максимально «чистый», то есть чтобы собственный шум усилителя был представлен в выходном напряжении ОУ в минимальной степени, нам требуется минимизировать коэффициент шума *NF*, определяющий вклад собственных шумов усилителя в выходной сигнал:

$$NF = 1 + \frac{P_a}{P_t},$$

где P_a – мощность собственных шумов усилителя, P_t – мощность теплового шума, генерируемого активной составляющей сопротивления входной цепи.

Считая полосы всех шумов и коэффициент усиления для всех шумов одинаковыми, можем выразить *NF* через параметры источников шума:

$$NF = 1 + \frac{\frac{e_a^2}{R} + i_a^2 R}{4kT}.$$

И, если мы при заданных e_a и i_a выбрали значение *R*, минимизирующее *NF*, то зная требуемое значение U_o, мы сможем рассчитать требуемый коэффициент усиления K_U.

Приведём ещё раз эквивалентную схему генератора шума на рисунке П6.

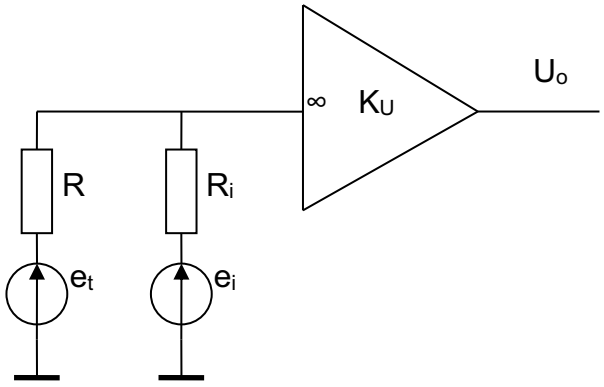


Рисунок П6 – Эквивалентная схема генератора.

Здесь R – сопротивления шумящего резистора, генерирующего ЭДС e_t, R_i – входное сопротивление усилителя, генерирующее ЭДС e_i.

В соответствии с законом Ома для полной цепи наибольшую мощность от источника R можно отобрать при условии $R_i = R$.

Таким образом, наилучшим вариантом следует считать первую схему, в которой (при достаточно больших сопротивлениях резисторов R_f) соблюдается равенство сопротивлений источника и приёмника, поскольку резисторы R в цепи каждого входа одновременно представляют выходные сопротивления источников термального шума и входные сопротивления усилителя.