– Во-вторых, это вычисление кратной точки некоторой эллиптической кривой над большим конечным полем $\mathbb{F}$

$E_{a,b}(p) = \{(x, y)|\ x, y \in \mathbb{F}, y^2 = x^3 + ax + b\ (\mathbb{F})\}$.

Пусть $P = (x, y) \in E_{a,b}(\mathbb{F})$ – точка большого порядка кривой $E_{a,b}(\mathbb{F})$, тогда функции $f(n)$ и $g(n, Q)$ определяются как $f(n)$: $\mathbb{Z}_q \to E_{a,b}(\mathbb{F})$, где $q = |<P>|$ – порядок циклической подгруппы, порожденной точкой P в группе $E_{a,b}(\mathbb{F})$, функция $g(n, Q)$: $\mathbb{Z}_q \times E_{a,b}(\mathbb{F}) \to E_{a,b}(\mathbb{F})$, такова, что значениями обеих функций $f(x)$ и $g(x, y)$ будут точки кривой $E_{a,b}(\mathbb{F})$ $f(n) = nP = P+P+...+P$; $g(n, f(m)) = n(mP) = mP+mP+...+mP = (mn)P$,и общий секрет пары также будет точкой $E_{a,b}(\mathbb{F})$ и вычисляется по формуле $K = g(n, f(m)) = n(mP) = g(m, f(n)) = m(nP) = (mn)P$.

Этот общий секрет представляется элементом циклической подгруппы $<P>$ группы точек кривой $E_{a,b}(\mathbb{F})$ над полем $\mathbb{F}$, порожденной точкой P, выбираемой так, что порядок группы $|<P>| = q$ – также большое простое число. Такой протокол обозначается как ECDH [4, 5]. Главный недостаток оригинального протокола Диффи-Хеллмана (DH) и его модификации ECDH, – отсутствие аутентификации сторон [3–5]. Поэтому за 45 лет предложено несколько вариантов усложнения этого протокола для получения протокола выработки общего секрета (ключа, аутентификатора) с взаимной аутентификацией сторон [4, 6–10].

В работах [1, 2] предложен новый общий метод формирования общего секрета (ключа, кода, аутентификатора) парой пользователей информационной системы (в частности, сети интернет), радикально расширяющий известные варианты протокола Диффи-Хеллмана и его обобщений, как его оригинального варианта, так и его модификаций с взаимной аутентификацией сторон или с аутентификацией только одной из них.

В данной работе мы реализуем один из вариантов этого метода, основанный на использовании новых арифметических операций в кольце показателей дискретной экспоненты или кольце кратностей выделенной точки эллиптической кривой над большим конечным полем, базирующихся на использовании одного конкретного класса легко реализуемых подстановок – класса взаимно однозначных дробно-линейных преобразований.

Предлагаются функции $f(x)$, $g(x, y)$ построенные на взаимно однозначном дробно-линейном преобразовании в показателях дискретной экспоненты над большим простым полем $\mathbb{Z}_p$, или взаимно однозначном дробно-линейном преобразовании в показателе кратности некоторой заданной заранее точки $P \in E_{a,b}(\mathbb{F})$ в группе точек эллиптической кривой над большим конечным полем $\mathbb{F}$, $E_{a,b}(p) = \{(x, y)|\ x, y \in \mathbb{F}, y^2 = x^3 + ax + b\ (\mathbb{F})\}$.

Идея использования дробно-линейного взаимно однозначного преобразования именно для этой цели была впервые высказана в работах первого из авторов настоящей статьи [1, 2].

Протокол DHFL.

Поскольку новая операция умножения $\otimes$ ассоциативна, то возможна перестановка скобок, а перестановкой скобок доказывается равенство:

$$K = K1 = Q2 \otimes Q2 \otimes \ \otimes Q2 = K2 = Q1 \otimes Q1 \otimes \ \otimes Q1$$

Таким образом, получившийся алгоритм корректен.

Таблица 1.

Шаг	Информация *Алисы*	Информация *Боба*
1	Случайно выбирает $x1$ $x1 \in X$	Случайно выбирает $x2$ $x2 \in X$
2	Вычисляет элемент $Q1 = g \otimes g \otimes \ \otimes g$ *«умножая его»* $x1$ раз	Вычисляет элемент $Q2 = g \otimes g \otimes \ \otimes g$ *«умножая его»* $x2$ раз
3	Получает от партнера $Q2 = g \otimes g \otimes \ \otimes g$ *«умноженный»* $x2$ раз	Получает от партнера $Q1 = g \otimes g \otimes \ \otimes g$ *«умноженный»* $x1$ раз
4	Вычисляет элемент $K1 = Q2 \otimes Q2 \otimes \ \otimes Q2$ *«умножая его»* $x1$ раз	Вычисляет элемент $K2 = Q1 \otimes Q1 \otimes \ \otimes Q1$ *«умножая его»* $x2$ раз

Литература

1. Лебедев, А. Н. Обобщенный протокол Диффи-Хеллмана с аутентификацией сторон / А. Н. Лебедев // Международная алгебраическая конференция, посвященная 110-летию со дня рождения профессора А. Г. Куроша. – М. : МГУ, 2018. – С. 123–127.

2. Лебедев, А.Н. Новая арифметика конечного коммутативного кольца и ее использование в криптографии / А. Н. Лебедев // Электронные информационные системы. – 2021. – Т. 30, № 3. – С. 49–63.

УДК 621.317.7

НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ ПАССИВНЫХ ФИЛЬТРОВ ДЛЯ ФОРМИРОВАНИЯ ОПОРНЫХ СИГНАЛОВ

Левко И.А.

Белорусский государственный университет
Минск, Республика Беларусь

Аннотация. Рассмотрен один из подходов к формированию опорных сигналов синусоидальной формы с использованием импульсных сигналов и пассивных ФНЧ. Показано, что реализация ФНЧ на практике требует не только проведения расчета с использованием специальных таблиц, но и применения программ моделирования электронных схем.

Ключевые слова: опорный синусоидальный сигнал, ФНЧ, нормированный фильтр, программа моделирования электронных схем.

SOME ASPECTS OF PASSIVE FILTERS APPLICATION FOR REFERENCE SIGNAL GENERATION

Levko I.

Belarusian State University
Minsk, Belarus

Abstract. One of the approaches to the sinusoidal reference signals generation using pulsed signals and passive low-pass filters is considered. It is shown that the implementation of a low-pass filter requires not only special design tables, but also the use of software electronic circuits simulator.
Key words: reference sinusoidal signal, LPF, normalized filter, electronic circuits simulator.

Адрес для переписки: Левко И.А., пр. Независимости, 4, г. Минск 220030, Республика Беларусь
e-mail: bsu@bsu.by

Опорные сигналы заданной формы, имеющие стабильную частоту, используются при решении ряда задач в измерительной технике и системах связи. Для формирования таких сигналов применяются специализированные аналоговые генераторы, а также цифро-аналоговые преобразователи, работающие в составе цифровых систем, решающих указанные задачи. В последнем случае для устранения высокочастотных компонент сигнала, появление которых обусловлено частотой дискретизации и ее гармониками, используются фильтры низкой частоты (ФНЧ), обеспечивающие сглаживание формы опорного сигнала.

Существует ряд задач, в которых применяются гармонические сигналы с фиксированной амплитудой и частотой, например, при квадратурной модуляции/демодуляции, синхронном детектировании и т.п. В этом случае высокая частотная стабильность может быть обеспечена за счет преобразования импульсного периодического сигнала в синусоидальный с помощью ФНЧ. Частотная стабильность 10^{-6} и выше здесь достигается при использовании генератора на основе кварцевого резонатора для формирования тактовой частоты.

Импульсный периодический сигнал содержит бесконечный ряд гармоник, кратных основной частоте, который может быть представлен в виде [1, с. 151]:

$$f(t) = \frac{1}{2}a_0 + \sum_{k=1}^{\infty} a_k \cos k\,\omega_1 t, \qquad (1)$$

где

$$a_k = 2U_0 \frac{T_0}{T} \frac{\sin \pi \rightleftarrows k \rightleftarrows T_0/T}{\pi \rightleftarrows k \rightleftarrows T_0/T}, \qquad (2)$$

U_0 – размах импульсного сигнала по напряжению; T_0 – длительность сигнала; T – период сигнала; $\omega_1 = 2\pi / T$ – базовая круговая частота или круговая частота первой гармоники. Для получения синусоидального сигнала из импульсного нужно обеспечить выполнение неравенства

$$a_1 >> a_n (n = 2, 3, \dots), \qquad (3)$$

т.е. амплитуда первой гармоники должна намного превосходить амплитуды высших гармоник. Этого можно добиться, используя ФНЧ. В случае произвольного соотношения между периодом T и длительностью T_0 импульсного сигнала процедуру фильтрации усложняет тот факт, что амплитуды высших гармоник, начиная со второй a_2, отличны от нуля.

Однако при выборе коэффициента заполнения 1/2, т.е. когда $T = 2T_0$, выражение (2) можно при-вести к виду

$$a_k = U_0 \frac{2}{\pi} \frac{1}{\rightleftarrows k \rightleftarrows}, k = 1, 3, 5, \dots \qquad (4)$$

Такой сигнал носит название меандр и обладает очень важным для решения поставленной задачи свойством: амплитуды гармоник с четными номерами у данного сигнала равны нулю, что существенно упрощает фильтрацию высших гармоник. Следует отметить также, что меандр достаточно просто получить в цифровых системах на практике.

Устройства аналоговой фильтрации можно разделить на два класса: пассивные и активные. Пассивные фильтры не позволяют усиливать сигнал, но обладают способностью работать с сигналами в диапазонах высоких и сверхвысоких частот. Активные фильтры строятся на усилительных элементах и поэтому могут усиливать сигнал, но имеют ограниченную полосу пропускания и, соответственно, работают в достаточно узком диапазоне частот.

Порядок фильтра определяется числом используемых реактивных элементов [2, с. 448]. Чем выше порядок фильтра, тем уже ширина полосы задерживания для получения нужной величины затухания A_s [3, с. 10].

Для различных типов фильтров частотные характеристики затухания могут отличаться как более, так и менее крутыми скатами.

Существует много схемотехнических решений фильтров ФНЧ. Среди них широкое распространение получили пассивные фильтры лестничного типа, содержащие емкостные и индуктивные реактивные элементы. При этом фильтр любого порядка, начиная со 2-го, формируется путем сочетания Г-, П- и Т-образных LC-секций [3, с. 35].

Для упрощения проектирования фильтров, рассчитанных на различные частотные диапазо-

ны, но имеющих одну и туже схемотехнику, применяется нормирование реактивных элементов фильтра для круговой граничной частоты 1 рад/с при активном сопротивлении нагрузки по входу и выходу 1 Ом.

Для решения задачи получения опорного сигнала определенный интерес представляют фильтры Баттерворта, благодаря линейности их фазовой характеристики. Следующим этапом после выбора типа фильтра, является определение его порядка. Для получения синусоидального сигнала очевидным критерием может служить соответствие заданному коэффициенту нелинейных искажений, который при использовании исходного сигнала типа меандр может быть описан приблизительной формулой:

$$k_{\text{н.и.}} \approx \frac{a_3}{a_1} \cdot 100\ \%, \qquad (5)$$

где a_1 и a_3 – амплитуды соответственно базовой и третьей гармоник в генерируемом сигнале. Для достижения $k_{\text{н.и.}}$ = 2 % отношение гармоник должно составлять 0,02 или –34 дБ. Согласно формуле (4) отношение указанных гармоник в исходном сигнале меандр составляет около –10 дБ. Отсюда затухание 3-ей гармоники за счет воздействия фильтра ФНЧ должно быть равно – 24 дБ. Этому критерию соответствует фильтр Баттерворта 3-го порядка [3, с. 92]. В данном случае фильтр может состоять из одной секции как П-, так и Т-образного типа. Единственным преимуществом схемы Т-образного типа (рис. 1) является вдвое меньший номинал катушки индуктивности, что обеспечивает несколько меньшие габариты, хотя это преимущество нивелируется необходимостью использования большего числа катушек индуктивности.

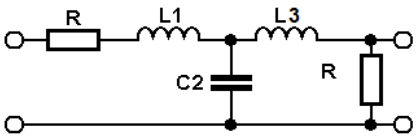

Рисунок 1 – Принципиальная схема Т-образного ФНЧ 3-го порядка

Нормированный фильтр-прототип имеет следующие значения элементов: $L_1 = L_3 = 1$, $C_2 = 2$. Для граничной частоты 500 кГц и активного сопротивления нагрузки 1,24 кОм действительные значения элементов оказываются равными $L_1 = L_3 = 395$ мкГн, $C_2 = 510$ пФ. АЧХ фильтра с данными значениями элементов приведена на графике №1 рис. 2.

Однако, на практике очень часто возникает несоответствие расчетных значений конденсаторов и индуктивностей и номиналов, доступных для использования. Это приводит к необходимости проверки того, насколько изменятся характеристики фильтра при отклонении номиналов элементов от расчетных.

Табличный подход, к сожалению, не позволяет производить обратный расчет, например, граничной частоты по имеющимся в наличии номиналам компонентов.

Выходом из данной ситуации может служить применение программ моделирования электронных схем. Так использование пакета программ LTspice компании Analog Devices Inc., находящийся в свободном доступе, позволило получить АЧХ фильтра, приведенного на рисунке 1, для различных значений элементов.

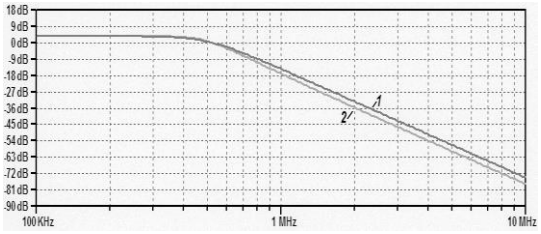

Рисунок 2 – АЧХ фильтра 3-го порядка для 2-х вариантов значений элементов

Так при сопротивления нагрузки 910 Ом и значении элементов $L_1 = L_3 = 390$ мкГн, $C_2 = 560$ пФ АЧХ фильтра, приведенная на графике №2 рисунка 2, изменяется незначительно и имеет более крутой скат, что является приемлемым

Литература

1. Корн, Г. Справочник по математике для научных работников и инженеров / Г. Корн, Т. Корн. – М.: Наука, 1973. – 832 с.

2. Белецкий, А. Ф. Теория линейных электрических цепей / А. Ф. Белецкий. – СПб. : Лань, 2017. – 544 с.

3. Ханзел, Г. Е. Справочник по расчету фильтров / Г. Е. Ханзел ; под ред. А. Е. Знаменского. – М. : Сов. радио, 1974. – 288 с.