ИССЛЕДОВАНИЕ ТОЧНОСТИ ИЗМЕРЕНИЯ ПЕРИОДА КОНФИГУРИРУЕМОГО КОЛЬЦЕВОГО ОСЦИЛЛЯТОРА

Трубач К. И., Иванюк А. А.
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: xenona11x@gmail.com, ivaniuk@bsuir.by

В работе изучается метод измерения периода конфигурируемых кольцевых осцилляторов (ККО) на FPGA Xilinx Artix-7. Эксперимент показывает, что при измерениях длительностью более 10^4 импульсов внутреннего генератора тактовой частоты погрешность составляет менее двух пикосекунд.

Введение

Одним из важнейших элементов аппаратной криптографии являются кольцевые осцилляторы (КО), используемые для идентификации цифровых устройств, генерирования криптографических ключей и последовательностей случайных чисел [1], а также для генерации последовательности прямоугольных импульсов на системах без встроенных кварцевых генераторов. Представленные в многочисленных конфигурациях, КО предоставляют различные периоды выходного сигнала, зависящие не только от схемы, но и от температуры, напряжения, давления и прочих факторов, в связи с чем возникает необходимость точно измерять их период. В данной работе рассматривается принцип проведения таких измерений с использованием временного окна, основанного на применении тактового сигнала известной частоты.

I. Конфигурируемые кольцевые осцилляторы

Применяемые в криптографии, КО используются как часть физически неклонируемых функций (ФНФ). При этом выделяется особая форма реализации этих устройств (ФНФ на базе КО, или КОФНФ), включающая большое количество КО для предоставления истинного случайного числа путём выбора некоторой функцией двух КО и дальнейшей обработкой их выходных сигналов. Однако такая схема обладает рядом недостатков, связанных с необходимостью реализовывать сложную функцию выбора, которая не является тривиальной. Эти проблемы решаются с помощью конфигурируемых кольцевых осцилляторов (ККО). Вместо выбора двух из множества КО, используется один ККО, предоставляющий уникальную частоту выходного сигнала каждой своей конфигурацией [2].

ККО реализуются большим количеством способов. Например, вместо нечётного количества инвертеров, классически используемых в КО, применяются двухвходовые вентили XOR, где один из входов служит для конфигурации. Вентили XOR могут заменять собой либо инвертеры, если на второй вход подаётся логическая единица, либо, при подаче логического нуля, буферы. Но требование к нечётности инвертеров, по сравнению с упомянутой ранее «классической» схемой, сохраняется и в этой, что влечёт необходимость использовать такое конфигурационное значение (challenge, или запрос), которое содержит в своём битовом представлении нечётное количество единиц. Это существенно ограничивает множество допустимых запросов.

Другой вариант схемы ККО, используемый в данной работе, предполагает использование мультиплексоров. Такая схема позволяет «выбирать» путь для сигнала кольцевого осциллятора подачей на управляющие входы мультиплексоров различных значений. Поскольку после реализации созданной схемы на FPGA возможно менять задержки только на соединительных элементах (но не на самих логических вентилях), такой подход предлагает высокую степень уникальности выходной последовательности и не ограничивает конфигурационное значение. Сама схема представлена на рис. 1, где C – запрос, En – сигнал, разрешающий работу ККО. В схему включён двухвходовой вентиль NAND, отвечающий за генерацию частоты, поскольку раз в некоторое время (зависящее от значения запроса) он инвертирует предыдущий сигнал, что и создаёт колебания.

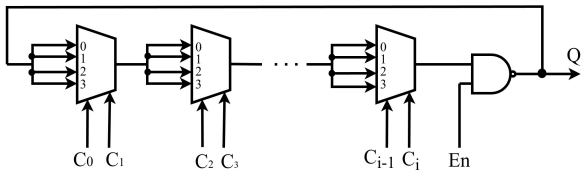

Рис. 1 – Структура ККО на базе мультиплексоров

II. Получение данных для исследования

Для того, чтобы измерить период ККО, необходимо иметь генератор с известной частотой. В рамках исследования, проводимого на FPGA Xilinx серии Artix-7, им выступает встроенный генератор тактовых импульсов частотой 100 МГц. На рис. 2 представлена схема, позволяющая отмерить необходимое время, т.е. число тактов встро-

Работа выполнена в совместной учебной лаборатории БГУИР-YADRO
https://www.bsuir.by/ru/kaf-informatiki/yadro

енного генератора, и получить количество тактов ККО, прошедших за это время, что и является основной исследуемой величиной.

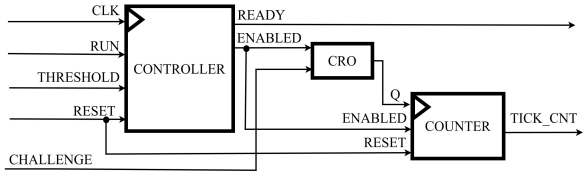

Рис. 2 – Структурная схема устройства измерения количества тактов ККО

Здесь блок контроллера (CONTROLLER), когда подан сигнал запуска (RUN), используется для обратного отсчёта от времени, заданного порогом (THRESHOLD), по внутреннему генератору тактовой частоты (CLK). Пока идёт отсчёт, разрешающий сигнал (ENABLED) активирует ККО и счётчик. По истечении этого времени счётчик и ККО останавливаются, и на выход схемы подаётся сигнал готовности (READY).

Будем называть экспериментом серию измерений для конкретных значений запроса и порога. Поскольку импульсы встроенного тактового генератора и последовательность, которую генерирует ККО, не синхронизированы, можно ожидать, что в рамках одного эксперимента со счётчика будет снято некоторое множество различных значений, что и повлечёт за собой погрешность измерения. Настоящее исследование определяет минимально необходимое окно для достаточно точного измерения периода осциллятора. С использованием предложенной схемы и некоторых запросов были собраны следующие данные: серия длиной 100 измерений для каждого порога от 1 до 65501 с шагом 100 единиц.

III. Анализ данных

Данные собирались в единицах тактов, а не в значениях периода, что позволяет избежать необходимости в дополнительной логике, связанной с вычислением значения периода при известной частоте синхронизации. Это минимизирует ошибки округления, так как перевод количества тактов в период может приводить к потере точности. Вместо этого можно выполнять умножение на дробные числа на заключительном этапе, что обеспечивает большую точность.

Поскольку длина серии в эксперименте достаточно большая, можно предполагать, что истинное значение периода ККО стремится к матожиданию периода всей серии. Тогда, полагая известными период системных часов T_{clk}, порог Thr_i и среднее арифметическое количества тактов ККО N_{avg_i} для i-го эксперимента, получим период ККО: $T_{cro} = \frac{T_{clk} \cdot Thr_i}{N_{avg_i}}$. Также, принимая количество тактов ККО в j–том измерении эксперимента как N_j, а длину серии в эксперименте как n, рассчитаем среднеквадратичную погрешность $S_i = \sqrt{\frac{\sum_{j=1}^{n}(N_j - N_{avg_i})^2}{n-1}}$ и ошибку периода $\xi = 0.5 \cdot \left(\frac{T_{clk} \cdot Thr_i}{N_{avg_i} - S_i} - \frac{T_{clk} \cdot Thr_i}{N_{avg_i} + S_i} \right)$. Итоговое выражение принимает форму $T_{cro} \pm \xi$. Очевидно, что, чем меньше ξ, тем более точным можно считать эксперимент. После проведения вычислений над данными при некотором значении запроса был получен график, представленный на рис. 3.

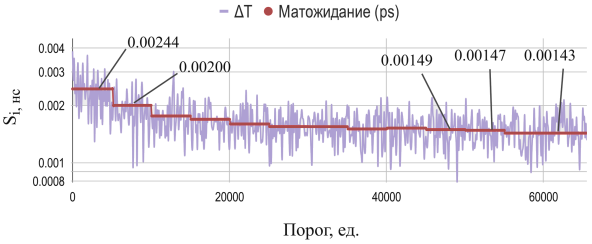

Рис. 3 – График зависимости среднеквадратичной погрешности от порога

Для каждых 50-ти значений порога было рассчитано значение матожидания (МО), показанное на графике ступенчатой линией. Линия выравнивается, говоря об уменьшении погрешности. Также приведены значения МО на некоторых отрезках. Когда значение порога начинает превышать 10^4 единиц, среднее значение погрешности опускается ниже двух пикосекунд (с относительной погрешностью 0.0167%), а, когда порог превосходит $4.5 \cdot 10^4$ единиц, МО приобретает ещё одну верную значащую цифру (значение $1.49 \cdot 10^{-3}$пс на графике составляет 0.01406% относительной погрешности). При этом обе ошибки всё ещё имеют одну верную значащую цифру – погрешность в одну пикосекунду, поэтому можно утверждать о том, что без существенных потерь в точности, но при её достаточности, в рассмотренной схеме для измерения периода ККО достаточно отсчитать не менее 10^4 импульсов встроенного генератора тактовой частоты.

IV. Выводы

По итогам данной работы экспериментально установлено, что при отсчете не менее 10^4 импульсов встроенного генератора тактовой частоты обеспечивается достаточная точность измерения периода ККО – относительная погрешность не превышает 0,0167%. Дальнейшее увеличение числа импульсов генератора до $4.5 \cdot 10^4$ повышает точность измерения периода ККО до 0,01406% относительной погрешности. Такие значения погрешности обеспечивают необходимую точность измерений, а предложенная схема устройства для измерений характеризуется простой в реализации структурой.

1. Иванюк А. А., Ярмолик В. Н. Конфигурируемый кольцевой осциллятор с управляемыми межсоединениями. Безопасность информационных технологий, 2024 / А. А. Иванюк, В. Н. Ярмолик. – Т. 31. – № 2. – с. 121–133.
2. Иванюк А. А., Ярмолик В. Н. Физически неклонируемые функции на базе управляемого кольцевого осциллятора. Безопасность информационных технологий, 2023 / А. А. Иванюк, В. Н. Ярмолик. – Т. 30. – № 3. – с. 90–103.