

Доклад / Технические науки - Электротехника, радиотехника, телекоммуникации, и электроника

Лосевской А.Ю.

**ИССЛЕДОВАНИЕ И АНАЛИЗ СХЕМ ИЗВЛЕЧЕНИЯ УНИКАЛЬНОЙ
ИНФОРМАЦИИ О КРИСТАЛЛЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ
ФУНКЦИЕЙ НА КОЛЬЦЕВЫХ ОСЦИЛЛЯТОРАХ В ПРИЛОЖЕНИИ К
ГЕНЕРАЦИИ КЛЮЧЕЙ ДЛЯ СИСТЕМ ШИФРОВАНИЯ**

*Московский Государственный Институт Электронной Техники,
Зеленоград, проезд 4806, д.5*

Losevskoy A.Y.

**ANALYSIS OF IC UNIQUE SEQUENCE EXTRACTION SCHEMES FOR
RING-OSCILLATOR PHYSICAL UNCLONEABLE FUNCTIONS IN
APPLICATION FOR CRYPTOGRAPHIC KEYS GENERATION**

National Research University of Electronic Technology, Zelenograd, passage 4806 5

Неизбежные случайные вариации параметров технологического процесса производства ИС приводят к тому, что каждая ИС по своей физической структуре является уникальной. Физически неклонированные функции (ФНФ) позволяют представить в виде двоичной последовательности уникальность ИС. Такие уникальные последовательности могут использоваться в качестве ключей в системах шифрования, в таком случае на них накладывается важное требование – они должны обладать воспроизводимостью в допустимом диапазоне изменения параметров функционирования ИС. В данной статье представлены схемы извлечения уникальных последовательностей, позволяющие снизить негативное влияние температурного фактора на воспроизводимость.

Ключевые слова: физически неклонлируемая функция, уникальная последовательность, кольцевой осциллятор, ключ системы шифрования.

Unavoidable random variations in the IC manufacturing process lead to the unique physical structures of every IC. Physical Uncloneable Functions allow binary representation of the IC uniqueness. These unique binary sequences can be used as cryptographic keys and in that case they must satisfy one of the most important requirements – the requirement of stability for the whole range of operation conditions. In this article a number of extraction schemes are present which allow reducing the impact of temperature on the binary sequence stability.

Key words: physical uncloneable function, unique sequence, ring oscillator, cryptographic key.

Введение

В настоящее время электронные устройства получили широкое распространение во многих сферах жизни человека. Люди полагаются на надежность и безопасность ИС, позволяя им управлять конфиденциальной информацией. Например, RFID метки могут использоваться в качестве ключей для доступа в здания, смарт-карты позволяют осуществлять финансовые операции, мобильные телефоны хранят такую уязвимую информацию, как личные документы, почту и т.п.

Для защиты конфиденциальной информации используются системы шифрования, позволяющие ограничить к ней доступ третьими лицами. При создании таких систем предполагается, что информация о секретных ключах злоумышленнику недоступна. Проблема хранения секретных ключей систем шифрования является одной из важнейших проблем, как с теоретической, так и с практической точки зрения.

В настоящее время для хранения секретных ключей систем шифрования используются различные виды постоянной памяти, например, память на пережигаемых перемычках или EEPROM. Для безопасного управления ключами в памяти порой приходится применять сложные и дорогостоящие решения. Постоянная память крайне уязвима к активным атакам с

проникновением. Такой вид атаки основан на изучении физической структуры микросхемы с использованием проникновения (например, послойный доступ к топологии устройства).

Для исключения такого рода атак ИС должна иметь активную защиту, использующую бесперебойное питание, что в конечном итоге приводит к высокой стоимости конечного устройства.

Инновационным способом безопасного хранения ключей является использование физически неклонированных функций (ФНФ). ФНФ позволяет создавать ключи для систем шифрования на основе уникальной информации, содержащейся в сложной физической структуре ИС, при этом, ключи «существуют» только во время работы ИС, что позволяет отказаться от их хранения в постоянной памяти.

ФНФ на кольцевых осцилляторах

Существуют различные варианты реализации ФНФ ([1], [2], [3], [4]). В случае использования уникальных последовательностей для генерации ключей систем шифрования наиболее подходящим вариантом является кремниевая ФНФ на кольцевых осцилляторах. Предпочтение было отдано данному варианту ФНФ не случайно: во-первых, такая ФНФ не требует внесения изменений в технологический маршрут производства ИС; во-вторых, она позволяет получать уникальные последовательности с наибольшей степенью воспроизводимости (в сравнении с остальными вариантами кремниевых ФНФ).

ФНФ на кольцевых осцилляторах впервые была предложена учеными Сух (Suh) и Деядас (Devadas) в совместной работе [1].

Экстракторами уникальной информации являются топологически идентичные кольцевые осцилляторы, представляющие собой комбинационные петли, на частоты осцилляций которых оказывают влияние вариации технологических параметров процесса производства ИС. Частоты осцилляций можно определить, подсчитывая число импульсов за фиксированный промежуток времени. Упрощенная конструкция ФНФ, состоящая из кольцевых осцилляторов, представлена на рис.1. Для извлечения уникальной информации

частоты кольцевых осцилляторов попарно сравниваются (сдвоенный мультиплексор выбирает пару осцилляторов). В результате сравнения частот каждой пары извлекается один бит уникальной информации.

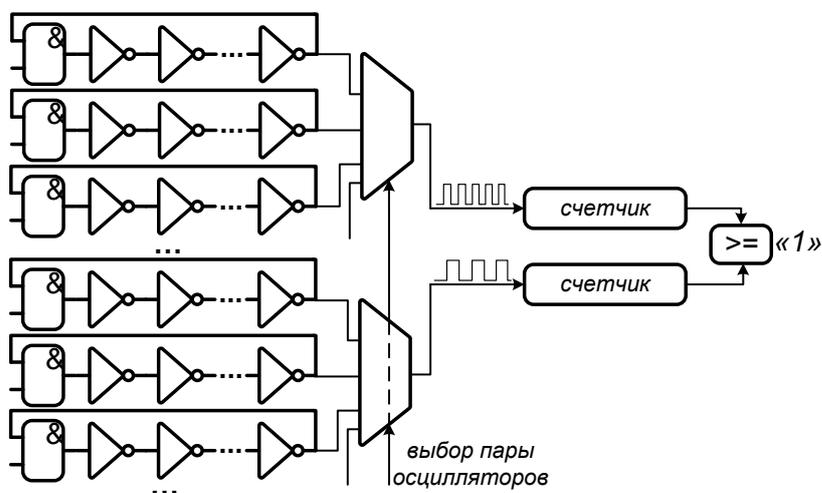


Рис.1. Конструкция ФНФ на кольцевых осцилляторах.

Уникальная последовательность может быть преобразована в ключ желаемой длины посредством операции хеширования. Если система шифрования накладывает определенные требования на используемые в ней ключи (например, ключевая пара алгоритма RSA), тогда хешированная уникальная последовательность используется в качестве заправки для алгоритма генерации ключей.

Математическая модель ФНФ на кольцевых осцилляторах

Рассмотрим два осциллятора a и b , результатом сравнения частот которых является уникальный бит. Суммарные задержки осцилляторов можно определить следующим образом:

$$d_a = d_{AVG} + d_{PVa} + d_{NOISEa}, \quad (1)$$

$$d_b = d_{AVG} + d_{PVb} + d_{NOISEb}, \quad (2)$$

где d_{AVG} определяет вклад в задержку одинаковый для всех осцилляторов ИС. Компоненты d_{PVa} и d_{PVb} обусловлены влиянием вариаций технологического процесса и считаются постоянными величинами при заданных параметрах окружающей среды (например, температура, влажность, напряжение питания и др.). Компонент d_{NOISE} связан с шумами, обусловленными нестабильностями в схеме (например, напряжения ИС могут флуктуировать в процессе измерения,

что приводит к изменению задержек), и по своей природе является динамически изменяющейся величиной. Величины d_{PV} и d_{NOISE} являются случайными и в выражениях (1) и (2) могут принимать как положительные, так и отрицательные значения.

Таким образом, значение уникального бита определяется знаком разности задержек осцилляторов:

$$d_a - d_b = (d_{PVa} - d_{PVb}) + (d_{NOISEa} - d_{NOISEb}) = \Delta d_{PV} + \Delta d_{NOISE}. \quad (3)$$

Предположим, что шумы вызванные нестабильностями в ИС отсутствуют, т.е. $\Delta d_{NOISE} = 0$. Тогда значение уникального бита при заданных условиях функционирования, будет определяться знаком Δd_{PV} . На практике неизбежно влияние нестабильностей в ИС на результаты измерений. В таком случае, если частоты осцилляторов достаточно близки ($|\Delta d_{PV}|$ мало), тогда наличие шумов при выполнении условия $|\Delta d_{NOISE}| \geq |\Delta d_{PV}|$ может приводить к неустойчивости уникального бита.

Кроме того, согласно теории на частоты осцилляторов влияют параметры окружающей среды. В том случае, если все осцилляторы являются идентичными (отсутствует разброс технологических параметров, т.е. $|\Delta d_{PV}| = 0$), тогда изменение их частот будет одинаковым. В действительности же осцилляторы таковыми не являются и законно предположить, что изменение параметров окружающей среды будет сопровождаться изменением величины $|\Delta d_{PV}|$.

Рассмотрим влияние температуры на воспроизводимость последовательности. Пусть при комнатной температуре осцилляторы A и B генерируют устойчивый бит ($|\Delta d_{PV}| > |\Delta d_{NOISE}|$), значение которого лог. «0». С повышением температуры частоты обоих осцилляторов будут уменьшаться (задержки d_a и d_b соответственно увеличиваются), но скорость изменения частот будет различаться. Для определенности положим, что частоты осцилляторов сближаются ($|\Delta d_{PV}|$ уменьшается). Если величина $|\Delta d_{PV}|$ была малой при комнатной температуре, то при некотором значении температуры T_{flip} разность $d_a - d_b$ изменит знак, что приведет в свою очередь к изменению

значения бита (рис.2б). Таким образом, уникальный бит является неустойчивым в диапазоне температур от T_1 до T_2 . Неустойчивость, связанная

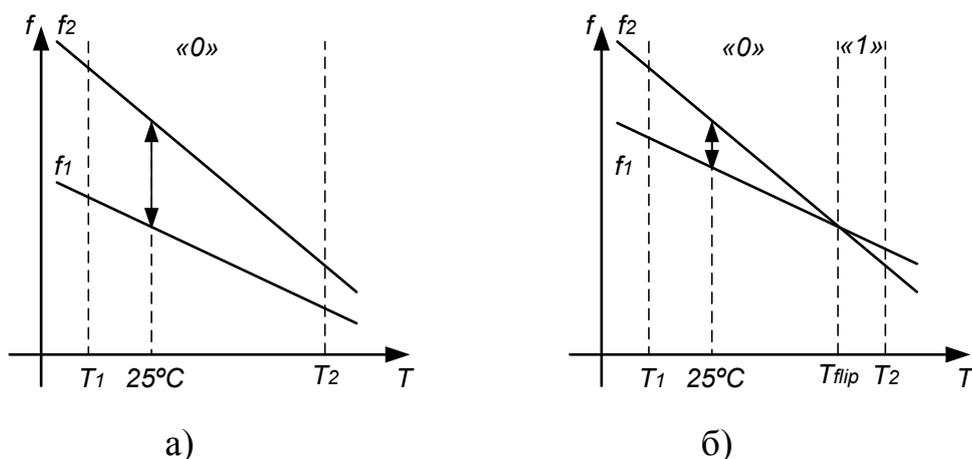


Рис.2. Бит устойчивый, т.к. пара имеет достаточный запас $|\Delta d_{PV}|$ (а), в противном случае пара генерирует неустойчивый бит (б).

с шумами в ИС, а также неустойчивость, вызванная различием скоростей изменения частот осцилляторов, получили название *флип-эффекта*.

Становится очевидным, что для повышения устойчивости уникальных бит (а значит и воспроизводимости последовательности в целом) необходимо увеличивать величину $|\Delta d_{PV}|$ для пары кольцевых осцилляторов и уменьшать величину $|\Delta d_{NOISE}|$ (рис.2а).

Математический аппарат оценки качества последовательностей

Два основных фактора определяющих качество последовательностей – *уникальность* и *воспроизводимость*.

Уникальность отражает степень уникальности последовательностей разных ИС. Оценкой уникальности служит среднее межчиповое значение расстояния Хэмминга (англ. Hamming Distance, HD) последовательностей. Предположим, что у нас есть две разные ИС u и v , и для них были получены последовательности R_u и R_v , каждая длиной n -бит. Тогда для ИС m среднее межчиповое HD может быть определено по следующей формуле:

$$\frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^m \frac{HD(R_u, R_v)}{n}. \quad (4)$$

Данное выражение включает в себя HD всевозможных вариантов пар последовательностей разных ИС. Для идеального случая, когда ФНФ

генерируют случайные уникальные последовательности, значение данного выражения равно половине длины ответа ($n/2$).

Непостоянство последовательностей, обусловленное проявлением флип-эффекта, отражается на воспроизводимости. Для ИС i при нормальных условиях функционирования (температура и напряжение питания) получаем n -битную последовательность R_i . Пусть R'_i - последовательность той же ИС, но полученная при условиях отличающихся от нормальных (изменяется температура и/или напряжение питания), при этом, генерацию последовательности повторяем x раз. Оценкой воспроизводимости будет являться среднее внутрочиповое расстояние Хэмминга по всем x последовательностям. Для i -й ИС выражение имеет следующий вид:

$$\frac{1}{x} \sum_{y=1}^x \frac{HD(R_i, R'_{i,y})}{n}, \quad (5)$$

где $R'_{i,y}$ - последовательность ФНФ i -й ИС при условиях функционирования y . Очевидно, что чем меньше внутрочиповое HD, тем выше воспроизводимость уникальной последовательности.

Теоретическое исследование схем извлечения

В работе [1] Деядас предлагает повышать воспроизводимость последовательностей посредством максимизации величины $|\Delta d_{PV}|$ для генерирующей пары. Для этого, пары объединяются в группы (ячейки) по n штук согласно определенным правилам, и в каждой выбирается пара с наибольшей разностью частот осцилляторов ее составляющих – такая пара и генерирует уникальный бит (назовем пару *лучшей*). Очевидно, что число ячеек определяется желаемой длиной уникальной последовательности. Метод получил название *схемы маскирования 1 из n*.

Рассмотрим три схемы извлечения – *простую схему, схему маскирования 1 из 3* и *схему маскирования 1 из 6*. Пусть все пары являются *независимыми* – каждый осциллятор участвует в создании только одной пары.

В простой схеме извлечения для генерации последовательности длиной в m бит необходимо $2m$ осцилляторов. Осцилляторы объединяются в *независимые* пары, которые и генерируют уникальные биты.

Применим аппарат теории вероятностей для оценки воспроизводимости уникальных последовательностей. Предположим, что в процессе образования пар осцилляторы выбираются случайным образом и вероятность того, что пара будет генерировать устойчивый бит во всем диапазоне изменения параметров окружающей среды, равна p . Пусть длина извлекаемой уникальной последовательности равна m бит, тогда вероятность того, что последовательность будет полностью воспроизводимой, определяется следующим выражением:

$$P_{stable} = p^m. \quad (6)$$

Рассмотрим схему маскирования 1 из 3. В такой схеме ячейка состоит из трех осцилляторов, и, таким образом, число возможных пар также равно трем. Следовательно, вероятность того, что в ячейке найдется хотя бы одна лучшая пара, будет определяться выражением:

$$p_{13} = 1 - (1 - p)^3. \quad (7)$$

Аналогично формуле (7) получим выражение для вероятности:

$$P_{stable13} = p_{13}^m = (1 - (1 - p)^3)^m. \quad (8)$$

В схеме маскирования 1 из 6 каждая ячейка состоит из четырех осцилляторов, что позволяет искать лучшую пару среди шести возможных. Аналогично предыдущему случаю, вероятность найти хотя бы одну лучшую пару будет равна:

$$p_{16} = 1 - (1 - p)^6. \quad (9)$$

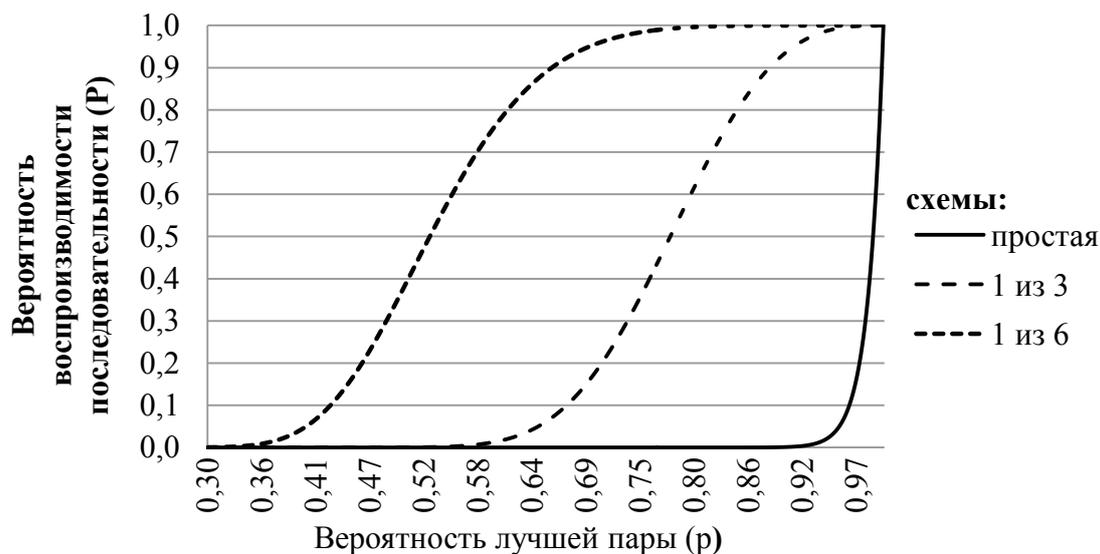


Рис.3. Зависимость вероятности воспроизводимости последовательности от вероятности лучшей пары.

Тогда вероятность воспроизводимости последовательности:

$$P_{stable16} = p_{16}^m = (1 - (1 - p)^6)^m. \quad (10)$$

Графики этих зависимостей для случая $m = 64$ представлены на рис.3. Как видно для обеспечения высокой вероятности воспроизводимости последовательности в случае простой схемы вероятность того, что пара является лучшей, должна быть достаточно высокой. В то же время, схемы маскирования позволяют ослабить требование к вероятности лучшей пары p . Так, например, для обеспечения 99%-ной вероятности устойчивости уникальной последовательности, вероятность p для простой схемы должна быть практически равной 1, для схемы 1 из 3 – 0,95, для схемы 1 из 6 – 0,77.

Деядас [1] рассмотрел схему маскирования 1 из 8. Для генерации уникальной последовательности длиной в 128 бит было использовано 1024 осциллятора. Пары объединялись в группы по 8, при этом некоторые из них могли быть *зависимыми*, т.е. иметь общие осцилляторы. Используя данную схему, он добился высокого уровня устойчивости последовательностей (99,32%) в диапазоне температур (от 20 до 120 °C).

Число осцилляторов необходимых для извлечения 128-ми битной уникальной последовательности приведено в табл.1. Очевидно, что

потребляемая мощность напрямую зависит от числа кольцевых осцилляторов (растет с увеличением их количества).

Таблица 1

Количество осцилляторов для схем извлечения

<i>Схема</i>	простая	1 из 3	1 из 6	1 из 8
<i>Кол-во осцилляторов</i>	256	384	512	1024

Таким образом, согласно теории, последовательность, извлеченная по схеме 1 из 6 должна иметь большую устойчивость в сравнении с последовательностями, полученными по простой схеме и схеме 1 из 3. Для проверки предположений был проведен эксперимент.

Экспериментальное исследование схем извлечения последовательностей

Результаты эксперимента позволяют получить информацию о воспроизводимости и уникальности последовательностей, полученных при использовании различных схем извлечения, и осуществить выбор оптимальной схемы.

Длина уникальной последовательности была выбрана равной 64-м битам из следующих соображений. Как было упомянуто ранее, среднее HD уникальных последовательностей составляет величину примерно равную половине длины последовательностей. Таким образом, для последовательностей длиной в 64 бита, среднее расстояние HD составляет 32 бита, что позволяет различать более 4 млрд. ИС (точное число 2^{32}). Используя хэш-функцию, уникальные последовательности преобразуются в ключи необходимой длины, причем вероятность того, что две ИС будут иметь одинаковые ключи чрезвычайно мала ($1/2^{32}$). Если же брать последовательность длиной в 32 бита, то число ИС имеющих различные ключи будет составлять величину немногим превышающую 66 тыс. (2^{16}), что не приемлемо при больших партиях ИС.

С точки зрения безопасности, если злоумышленнику удалось определить длину ключа системы шифрования, то время подбора ключа не будет зависеть от длины уникальной последовательности, из которой был получен ключ.

Таким образом, *выбор длины уникальной последовательности определяется размером партии ИС.*

В качестве платформы для исследования схем извлечения уникальных последовательностей была использована отладочная плата ML402 фирмы Xilinx с установленной на ней FPGA семейства Virtex-4 модели XC4VSX35 с эквивалентным числом логических элементов равным 34560. В ходе исследования было задействовано 9 отладочных плат ML402.

Блок-схема экспериментальной установки представлена на рис.4. Блок массива осцилляторов (БМО) содержит 256 кольцевых осцилляторов размещенных в массиве 4 на 64.

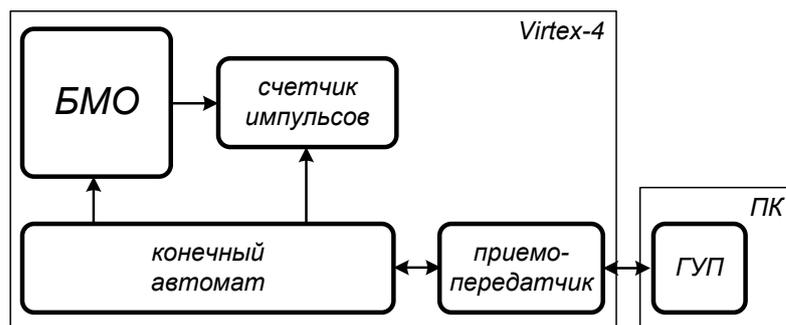


Рис.4. Структурная схема установки.

Кольцевой осциллятор представляет собой комбинационную петлю, осциллирующую с определенной частотой. Частота определяется как конструктивными особенностями петли, так и параметрами окружающей среды (например, температура и напряжение питания ядра). Кольцевой осциллятор, использованный в данной работе, состоял из семи стадий инверсии и одной буферной стадии, введенной для дополнительного уменьшения частоты осцилляций (рис.5). Все стадии были реализованы на основе логических генераторов (LUT). Каждый конфигурируемый логический блок (CLB) содержит 4 сектора (Slice): два сектора позволяют реализовывать только комбинационную логику (SliceL), и два сектора (SliceM) имеют расширенную функциональность, которая дает возможность создавать сдвиговые регистры и

распределенную память. В каждом Slice содержится по 2 LUT и, таким образом, общее число LUT в одном CLB равно 8, благодаря чему один кольцевой осциллятор полностью уместился в одном CLB. В таком случае обеспечивалась локальная трассировка всех стадий осциллятора.

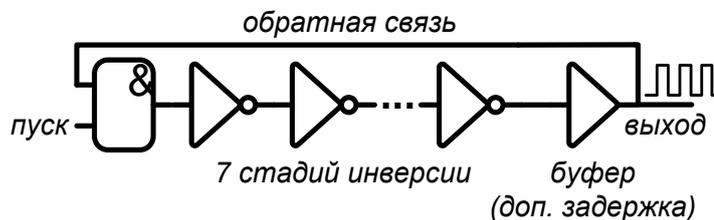


Рис.5. Структура кольцевого осциллятора.

Оценить минимальную частоту осцилляций можно по следующей формуле:

$$f_{\text{мин.}} = \frac{1}{T_{\text{макс.}}} = \frac{1}{2(8t_{LUT} + t_{\text{тр.}})}, \quad (11)$$

где t_{LUT} - время задержки на LUT, $t_{\text{тр.}}$ - время задержки на трассировке. Согласно спецификации на семейство микросхем Virtex-4 [5], максимальное значение t_{LUT} составляет величину 0,2 нс. Суммарное время задержки, которое вносит трассировка ($t_{\text{тр.}}$), можно определить, используя информацию о статистических значениях задержек предоставляемую программой Xilinx FPGA Editor. Величина $t_{\text{тр.}}$ оказалась равной 2,9 нс, и, таким образом, минимальная частота осциллятора $f_{\text{мин.}}$ равна 111 МГц.

Для обеспечения *топологической идентичности* кольцевых осцилляторов, был создан аппаратный макрос в программе Xilinx FPGA Editor. Использование макроса позволяет создавать на этапе размещения необходимое число топологически идентичных осцилляторов. Для того чтобы разместить осцилляторы в прямоугольный массив, были использованы ограничения на размещение.

Измерение частоты осцилляторов осуществлялось 20-ти разрядным *счетчиком импульсов*. Время подсчета импульсов равнялось 2 мс, таким образом, максимальная частота осциллятора, которую был способен измерить

счетчик, равнялась 520 МГц. Измерение частоты каждого осциллятора повторялось 50 раз.

Конечный автомат был использован для управления процессами подсчета импульсов осцилляторов и опправки результата (содержимого счетчика) на ПК для дальнейшей обработки.

Генератор уникальной последовательности (ГУП) представлял собой программную реализацию схем извлечения на языке Tcl.

Для исследования устойчивости последовательностей в температурном диапазоне от 85 до -45°C платы помещались в проходную камеру.

Простая схема извлечения. Для генерации 64-х бит уникальной последовательности при помощи простой схемы извлечения необходима информация о частотах 64-х пар кольцевых осцилляторов. Таким образом, общее число задействованных осцилляторов 128.

Уникальные последовательности для нормальных условий ($+25^{\circ}\text{C}$) были получены на основе усредненных значений частот осцилляторов (напомним, что измерение частоты каждого осциллятора повторялось 50 раз).

Гистограмма HD для последовательностей представлена на рис.6. Среднее значение HD оказалось равным 31,2 битам и отклоняется от идеального случая (32 бита) на 2,5%. Причиной этого может быть как неравное количество нулей и единиц в уникальных последовательностях, так и совпадение значений в битовых позициях последовательностей.

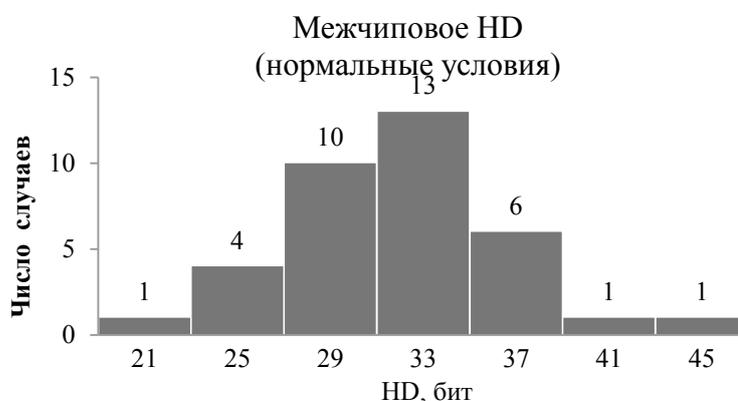


Рис.6. Гистограмма HD для уникальных последовательностей.

Воспроизводимость последовательностей можно оценить по внутрочиповому HD. Частоты осцилляторов, как и предполагалось, увеличиваются с понижением температуры. Как уже было упомянуто ранее, для обеспечения устойчивости бита, генерируемого парой осцилляторов, необходимо, чтобы разность частот этих осцилляторов сохраняла свой знак во всем температурном диапазоне (необходим достаточный запас $|\Delta d_{PV}|$). К сожалению, на практике данное условие выполняется не всегда. На рис.7а представлена температурная зависимость разности частот осцилляторов пары, генерирующей неустойчивый бит.

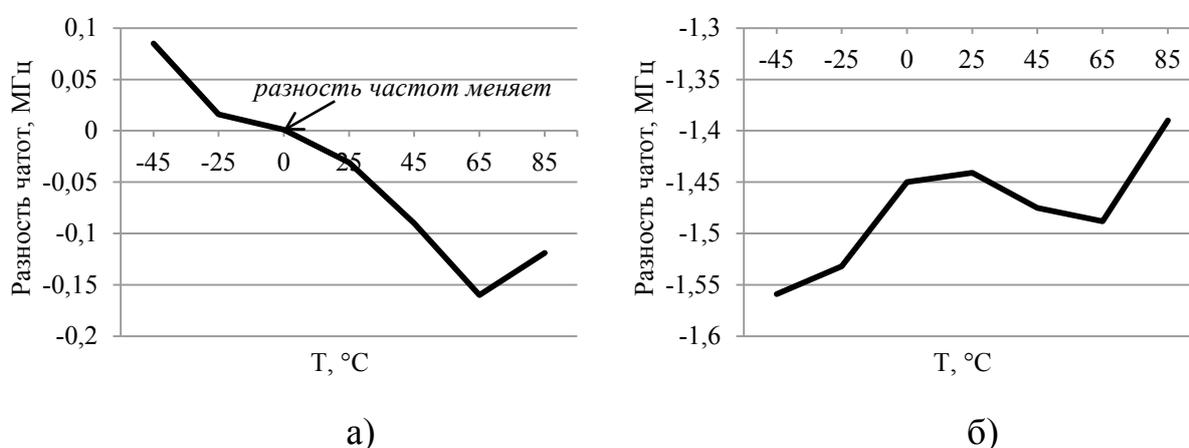


Рис.7. Разность частот пар генерирующих неустойчивый бит (а) и устойчивый бит (б).

Для сравнения, на рис.7б представлен аналогичный график для пары, которая генерирует стабильный бит во всем диапазоне температур.

Для оценки воспроизводимости уникальных последовательностей, был произведен расчет среднего значения внутрочипового HD для последовательностей ФНФ (рис.8). Расчет проводился относительно последовательностей полученных при нормальных условиях. Наблюдается увеличение числа неустойчивых бит при отклонении температуры окружающей среды от нормального значения. Максимальная величина среднего значения внутрочипового HD наблюдается у 4-й ФНФ при 85 °С и равна она 6,8 битам, что говорит о высокой вероятности возникновения 7-ми неустойчивых бит в последовательности при ее повторном извлечении.

С первого взгляда может показаться, что зависимость среднего значения HD отклоняется от ожидаемой тенденции – с понижением температуры воспроизводимость последовательностей ФНФ не увеличивается. Связано это с тем, что смена знака разности частот пар осцилляторов происходит при различных температурах.

Для устранения ошибок в последовательностях, необходимо использовать системы коррекции ошибок. Данная схема извлечения требует сложные корректирующие коды, способные исправлять большое число ошибок.

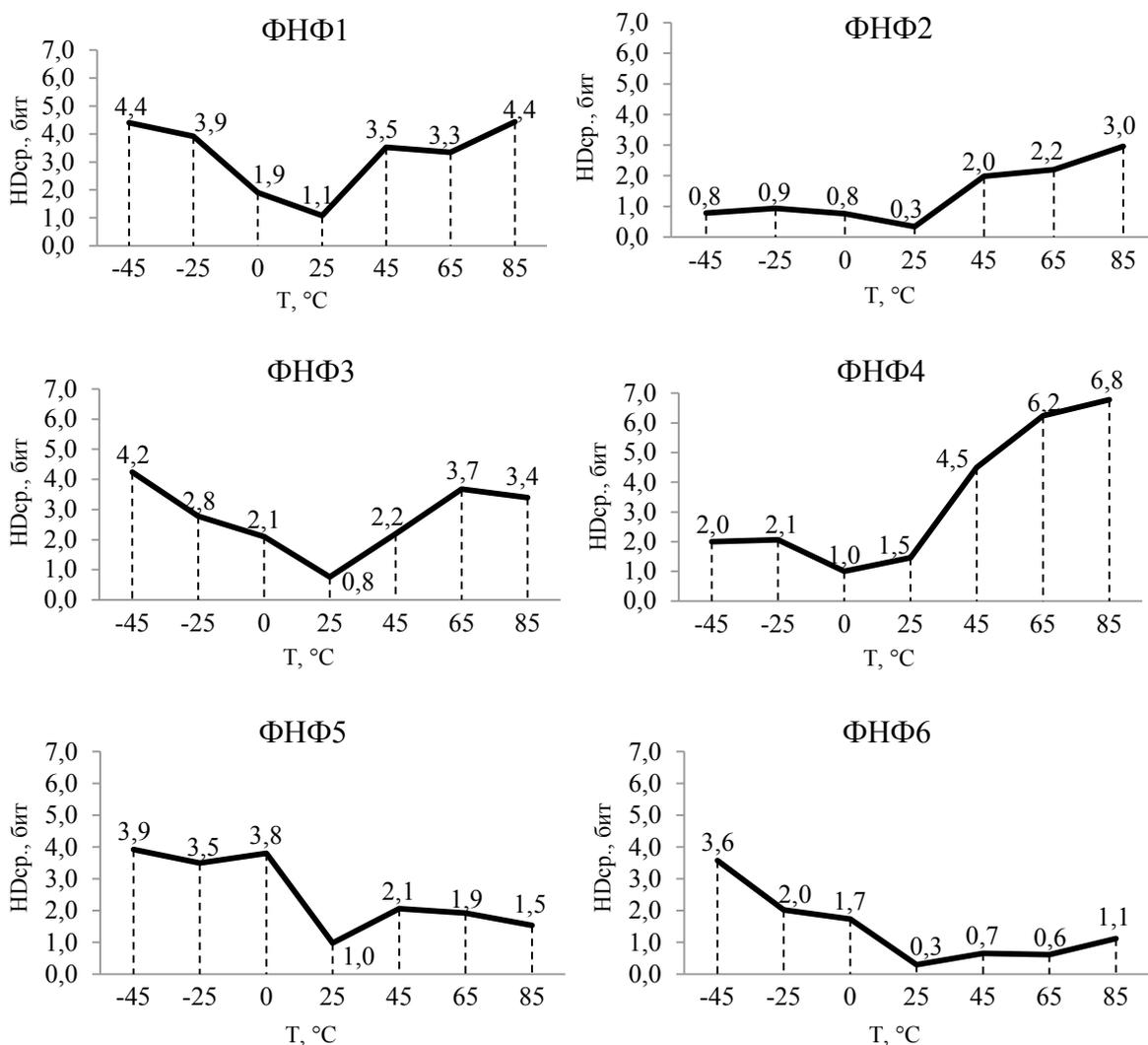


Рис.8 (начало).

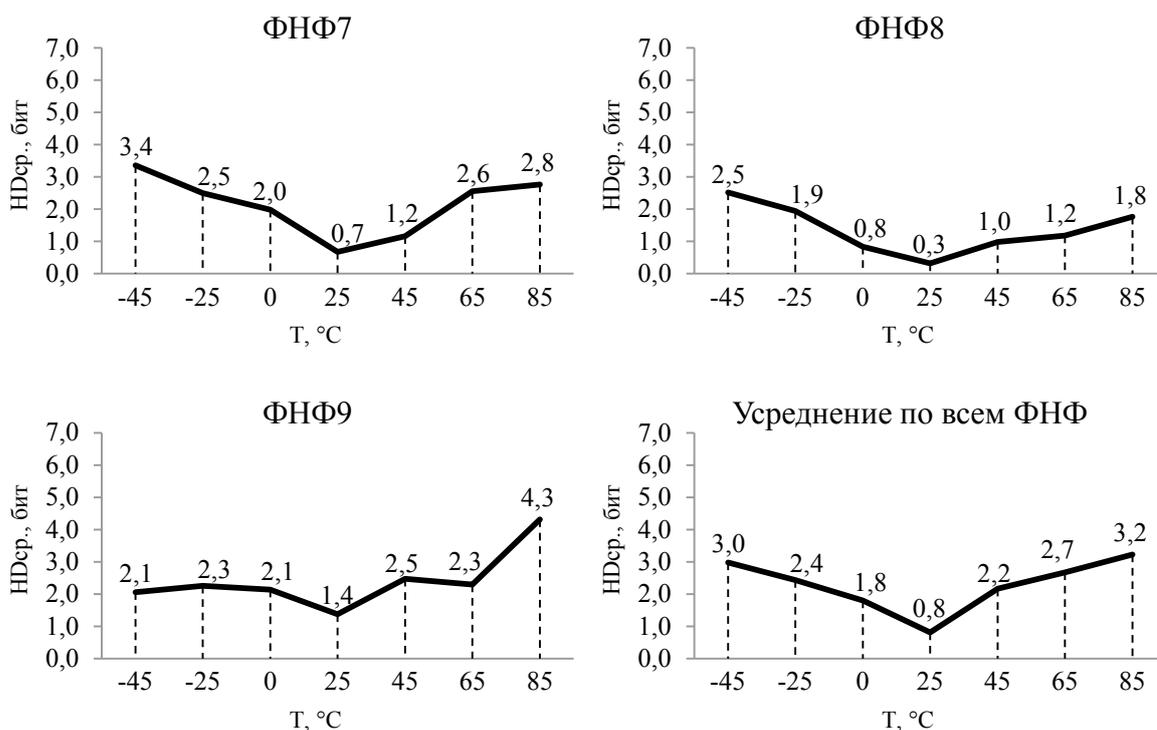


Рис.8 (продолжение). Зависимость от температуры среднего значения внутричипового HD уникальных последовательностей ФНФ для простой схемы.

Схема маскирования 1 из 3. Теперь для извлечения 64-х битных последовательностей общее число задействованных осцилляторов равно 192. Поскольку в каждой ячейке содержится по 3 осциллятора, общее число возможных пар равно 3-м, и, таким образом, появляется возможность выбора лучшей пары осцилляторов имеющей наибольшую разность частот (рис.9).

Извлечение уникальной последовательности ИС в случае использования схем маскирования осуществлялось в два этапа [1]. В процессе *инициализации*

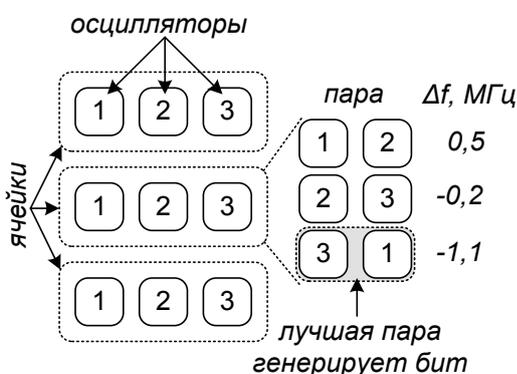


Рис.9. Ячейка с осцилляторами в схеме маскирования 1 из 3.

извлекалась уникальная последовательность, которая признается истинной, не содержащей ошибок. При этом номера лучших пар сохранялись и в дальнейшем использовались в процессе *регенерации* для наиболее точного восстановления исходной последовательности.

Истинные уникальные последовательности, как и для простой схемы извлечения, были получены в нормальных условиях. На рис.10 представлена гистограмма межчипового HD этих последовательностей для 9-ти ФНФ. Среднее значение HD равно 31,5 бита и отличается от идеального случая (32 бита) на 1,6%.

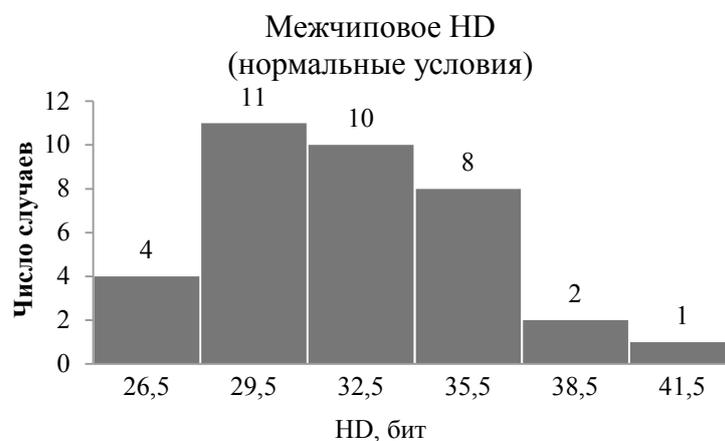


Рис.10. Гистограмма HD для уникальных последовательностей.

Наблюдается значительное повышение степени воспроизводимости уникальных последовательностей (рис.11). В нормальных условиях все уникальные последовательности имели среднее значение внутричипового HD равное 0,0 бита, что говорит о малой вероятности появления неустойчивых бит. Максимальное отклонение от истинной последовательности имеет последовательность 5-й ФНФ при -45 °С, и составляет 2,8 бита, что говорит о высокой вероятности возникновения 3-х неустойчивых бит.

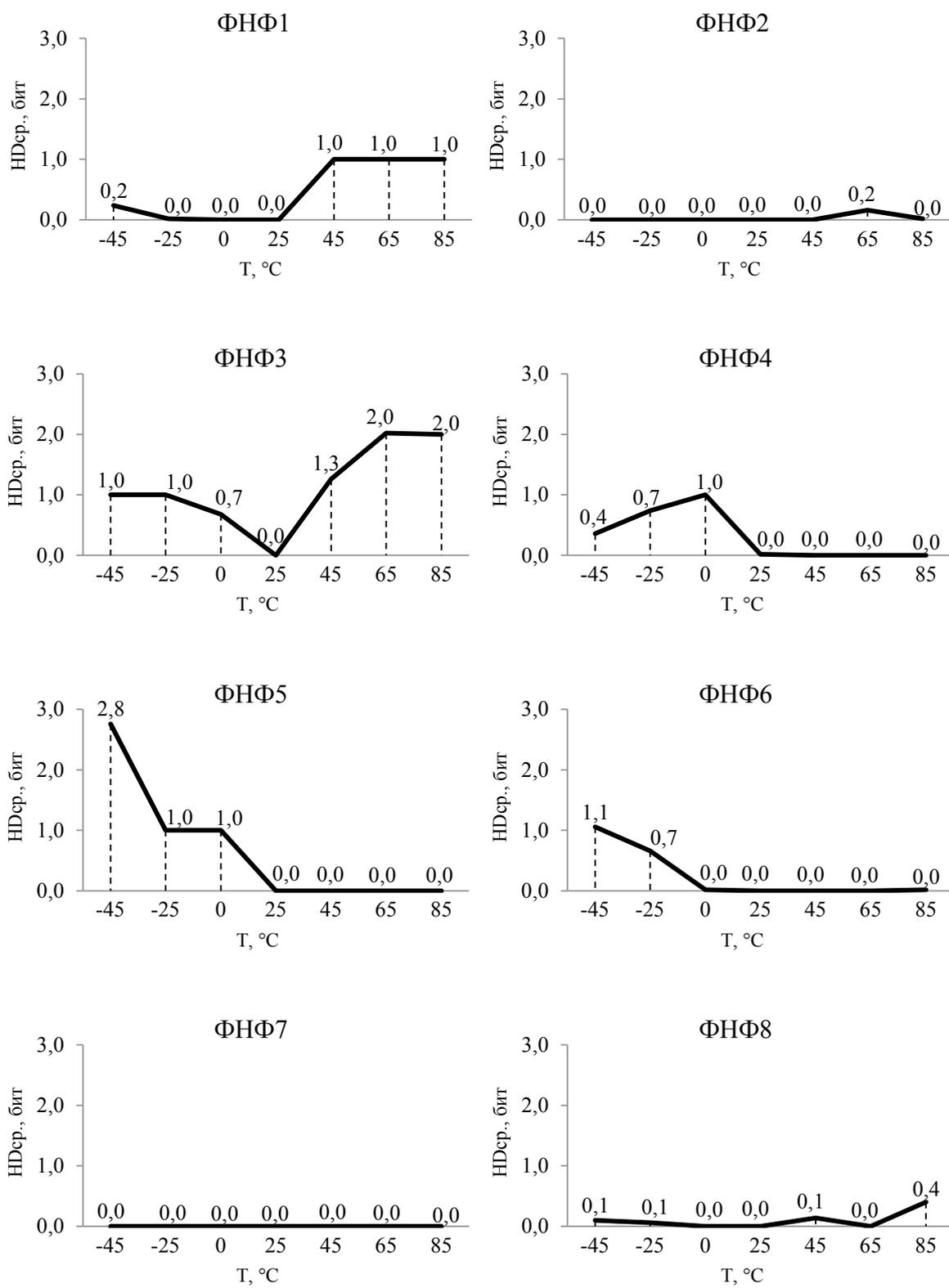


Рис.11 (начало).

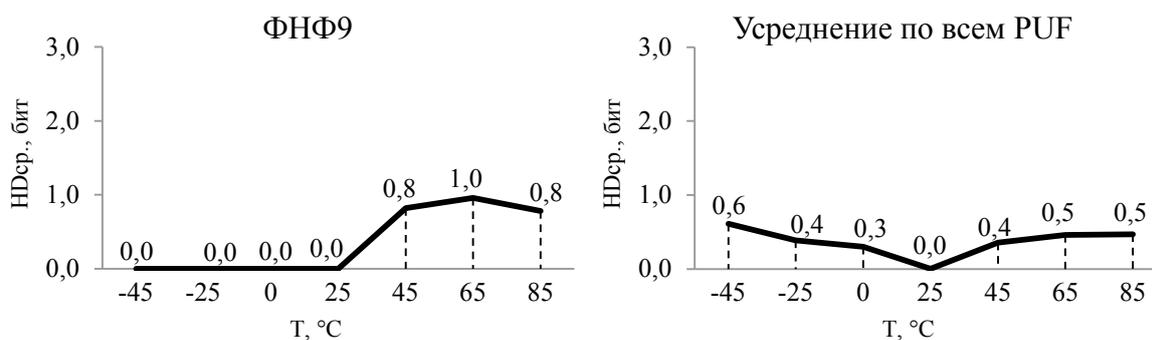


Рис.11 (продолжение). Зависимость от температуры среднего значения внутрочипового HD уникальных последовательностей ФНФ для схемы маскирования 1 из 3.

Для диапазона температур от -25 до +65 °C вероятность возникновения более 2-х неустойчивых битов мала. Поэтому, можно использовать корректирующие коды способные исправлять до 2-х ошибок. Для расширения температурного диапазона необходимы более мощные коды.

Схема маскирования 1 из 6. Отличие от предыдущей схемы маскирования заключается лишь в числе осцилляторов в ячейке. В данном случае ячейка состоит из 4-х осцилляторов, и общее число вариантов пар увеличивается до 6-ти (аналогично рис.9). Для генерации 64-х битных последовательностей необходимо 256 кольцевых осцилляторов.

Гистограмма межчипового HD для истинных уникальных последовательностей представлена на рис.12. Среднее значение HD равно 32,6 битам и отличается от идеального случая (32 бита) на 1,9%.

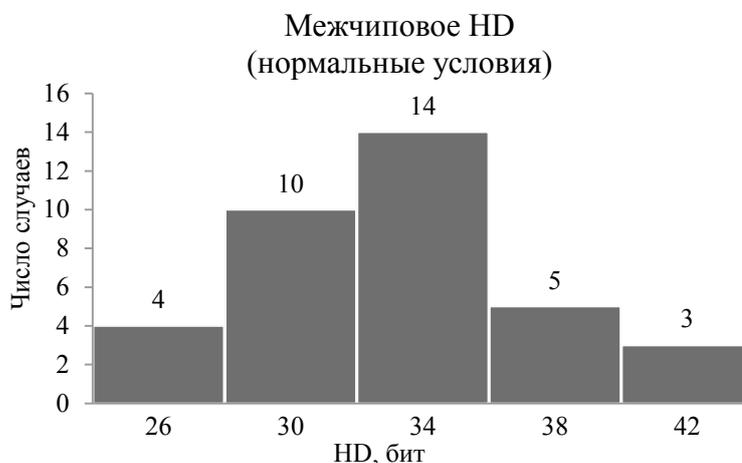


Рис.12. Гистограмма HD для уникальных последовательностей.

Данная схема извлечения позволяет повысить устойчивость уникальной последовательности, поскольку возрастает вероятность существования лучшей пары. На рис.13 приведены графики подтверждающие это.

Максимальное значение внутрочипового HD у 8-й ФНФ и равно 1,8 битам, что указывает на высокую вероятность появления двух неустойчивых бит в процессе регенерации последовательности. Тем не менее, у большинства ФНФ среднее число неустойчивых битов оказалось близким к 0,0 битам, что говорит о высокой степени воспроизводимости последовательностей этих ФНФ. Таким образом, используя корректирующие коды способные исправить две ошибки можно добиться восстановления уникальных последовательностей ФНФ во всем диапазоне температур.

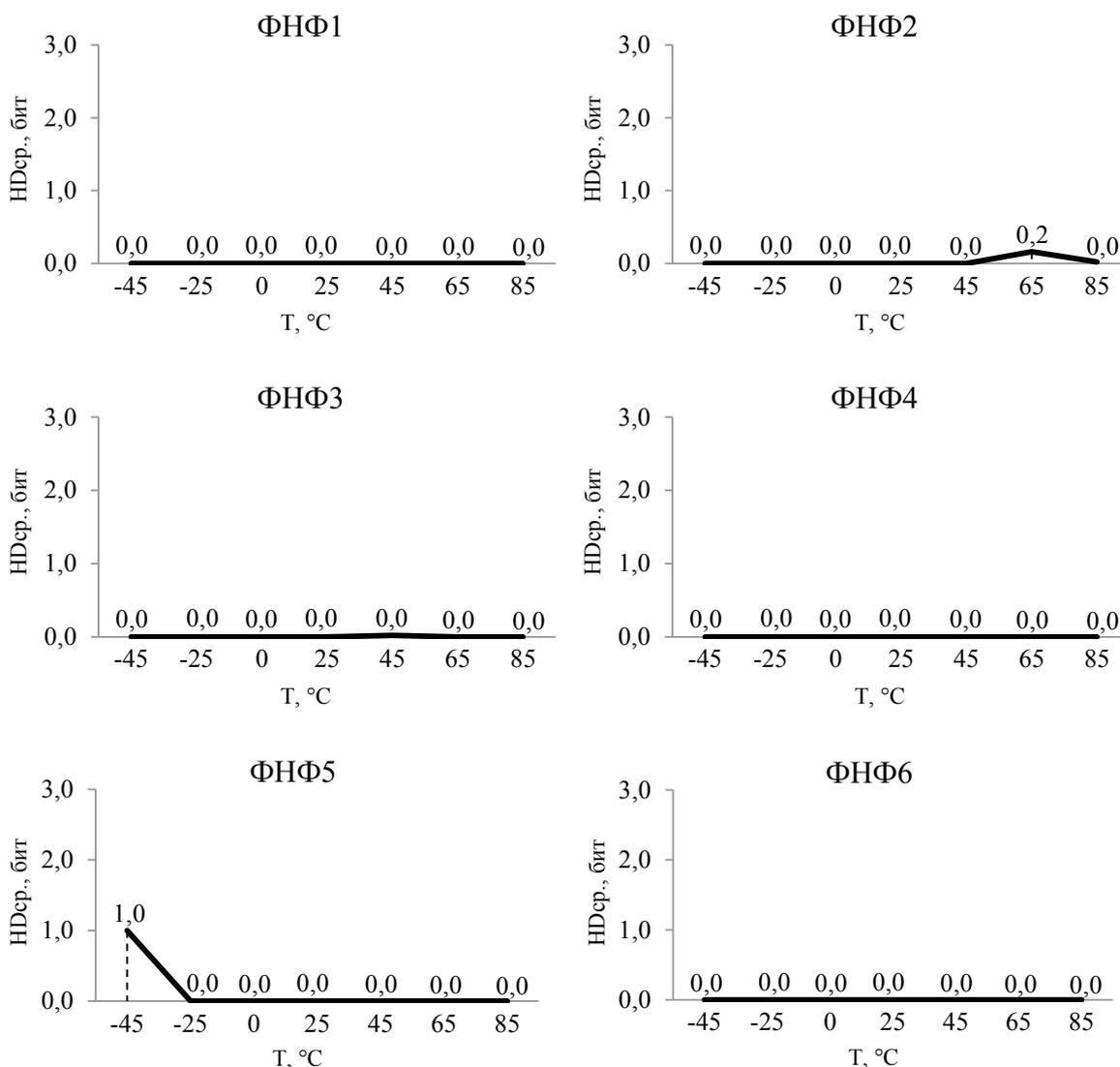


Рис.13 (начало).

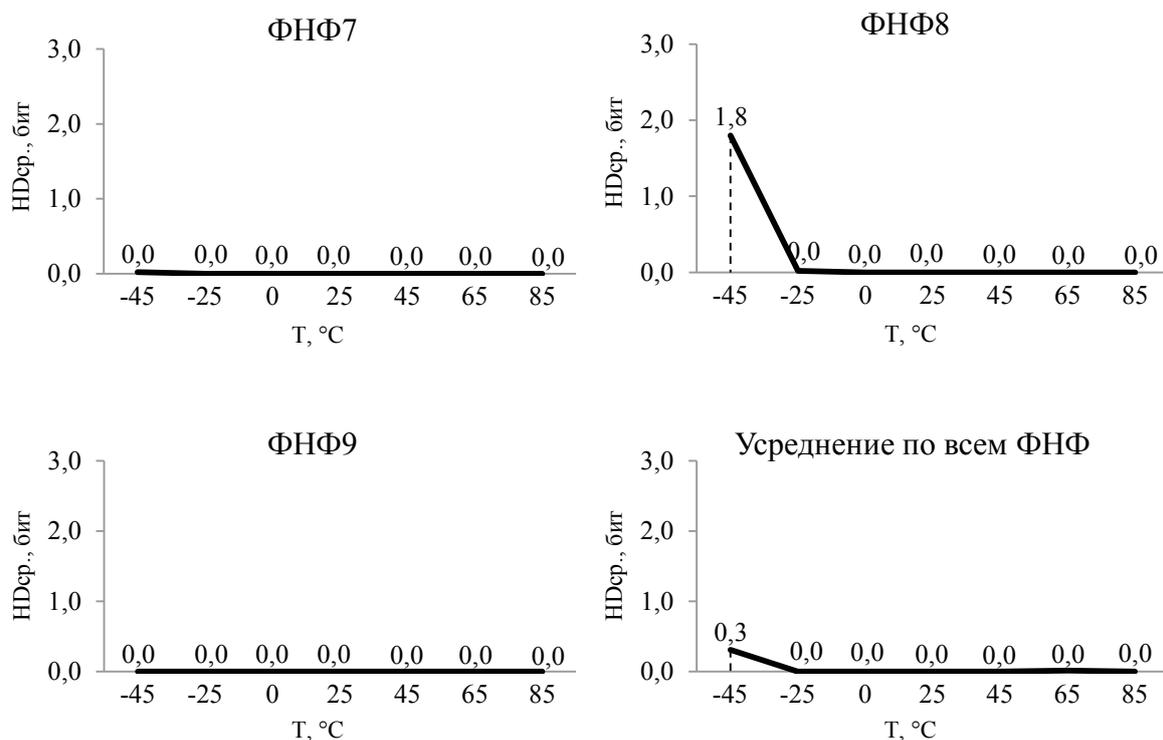


Рис.13 (продолжение). Зависимость от температуры среднего значения внутричипового HD уникальных последовательностей ФНФ для схемы маскирования 1 из 6.

Выбор оптимальной схемы маскирования. Эксперимент подтверждает предположения, выдвинутые в теории. Схема маскирования 1 из 6 позволяет добиться более высокой устойчивости последовательностей по сравнению со схемой маскирования 1 из 3 и схемой без маскирования.

Используя коды, исправляющие 2 ошибки, схема маскирование 1 из 3 может обеспечить устойчивую работу ФНФ в температурном диапазоне от -25 до +65 °С. Для перехода в температурный диапазон от -45 до +85 °С необходимо использовать коды, исправляющие 3 ошибки, реализация которых требует большего количества ресурсов. Альтернативным вариантом в таком случае может быть переход к схеме маскирования 1 из 6, которая обеспечит устойчивую работу в диапазоне от -45 до +85 °С, при использовании корректирующих кодов способных исправить 2 ошибки.

Заключение

В данной статье были исследованы и проанализированы схемы извлечения уникальных последовательностей ФНФ на кольцевых осцилляторах. Предположения, выдвинутые в теории, были подтверждены экспериментально. Были даны рекомендации по выбору оптимальной схемы извлечения.

Несмотря на оптимистические результаты, предстоит еще проделать большой объем работы связанной с оптимизацией ФНФ. Необходимо подобрать оптимальное время измерения частот осцилляторов. В экспериментальном варианте каждый осциллятор измерялся в течение 2 мс. Слишком малое время измерения отрицательно сказывается на точности определения разности частот осцилляторов. Уменьшить время измерения при сохранении точности можно за счет повышения частот кольцевых осцилляторов (сократив число инвертирующих стадий), но при этом неизбежно возрастет мощность потребляемая устройством.

Литература:

1. G. Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In DAC. IEEE, 2007.
2. Sandeep S. Kumar, Jorge Guajardo, Roel Maes, Geert Jan Schrijen, and Pim Tuyls. The butterfly puf: Protecting ip on every fpga. In HOST. IEEE Computer Society, 2008.
3. M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure PUFs", in Proc. ICCAD, 2008.
4. Erdinc Ozturk, Ghaith Hammouri, Berk Sunar. Physical Unclonable Function with Tristate, Buffers. Worcester Polytechnic Institute, USA, 2007.
5. Virtex-4 FPGA Data Sheet: DC and Switching Characteristics (http://www.xilinx.com/support/documentation/data_sheets/ds302.pdf).

References:

1. G. Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In DAC. IEEE, 2007.
2. Sandeep S. Kumar, Jorge Guajardo, Roel Maes, Geert Jan Schrijen, and Pim Tuyls. The butterfly puf: Protecting ip on every fpga. In HOST. IEEE Computer Society, 2008.
3. M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure PUFs", in Proc. ICCAD, 2008.
4. Erdinc Ozturk, Ghaith Hammouri, Berk Sunar. Physical Unclonable Function with Tristate, Buffers. Worcester Polytechnic Institute, USA, 2007.
5. Virtex-4 FPGA Data Sheet: DC and Switching Characteristics (http://www.xilinx.com/support/documentation/data_sheets/ds302.pdf).