АНАЛИЗ СПОСОБОВ ПРЕСЕЛЕКЦИИ ЯЧЕЕК ПАМЯТИ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

Суханов С.В.
аспирант, МОУ «Институт инженерной физики», г. Серпухов
neron1987@mail.ru

Аннотация. *В статье рассматривается один из способов предварительной обработки ячеек физически неклонируемых функций (ФНФ), построенных на основе ячеек статического оперативного запоминающего устройства (СОЗУ) – параллелизация.*

Ключевые слова: *физически неклонируемые функции, ячейка статического оперативного запоминающего устройства, предварительная обработка, преселекция.*

ANALYSIS OF PHYSICALLY PRESELECTION MEMORY NON-CLONABLE FUNCTIONS

Suhanov S.V.
Postgraduate MOU "Institute of Engineering Physics", Serpukhov

Abstract. *The article describes one way to pretreatment of cells physically nekloniruemyh functions (FNF), built on the basis of cell static random access memory (SRAM) - parallelization.*

Keywords: *physically nekloniruemye function, cell static random access memory, pretreatment preselection.*

Введение

ФНФ – это физическая система (устройство), неотъемлемым свойством которой является неклонируемость (неповторяемость) некоторых ее функций, свойств, характеристик либо параметров [1]. ФНФ состоят из множества компонент, чьи параметры принимают случайные значений во время производства. Значениями параметров компонент, в процессе создания устройства, из-за их физической особенности невозможно управлять. При подаче сигнала на вход устройства формируется выходной сигнал (ответ) в виде значения случайного параметра компоненты, которое для разных устройств будет различным. Таким образом, каждое устройство является уникальным. Следовательно, нельзя получить два идентичных устройства, который при одном и том же входном сигнале формировали один и тот же ответ. ФНФ могут быть использованы во многих технологиях: смарт-карты, банковские карты, RFID-метки, и другие объекты, которые чаще всего подвержены процедуре подделывания.

В соответствии с проведенным анализом [2] многие реализации ФНФ на основе ячеек СОЗУ весьма ненадежны, т.к изменения параметров работы (вариация питания и температуры) сильно сказываются на стабильности ответов устройств. С целью увеличения надежности ответов используются способы предварительной обработки ячеек СОЗУ [3].

Теория

Предварительная обработка – это способы, с помощью которых сокращается частота появления ошибок во время некоторой процедуры на начальном этапе. Цель предварительной обработки – уменьшение частоты появления ошибок таким образом, что бы последующая коррекция ошибок становилось менее сложной или даже ненужным.

Кроме того, может быть необходимым резервирования ячеек ФНФ – это означает, что более одной ячейки ФНФ используется для формирования одного выходного бита. В контексте кодов коррекции ошибок, это значение было определено как избыточность

«R». В контексте предварительной обработки это называется эффективностью «e»:

$$e = \frac{o}{s}, \quad (1)$$

где o – количество выходных значений, s – число всех ячеек ФНФ

Чем выше эффективность, тем лучше подход с точки зрения расходов (площадь, мощность, …). Например, если для создания одного выходного бита необходимо 5 ячеек ФНФ, то коэффициент полезного действия (КПД)=20%.

Вторая интересная характеристика способов предварительной обработки является отношение между эффективностью и стабильностью. Как правило, чем выше эффективность, тем ниже стабильность. Это соотношение показано на рисунке 1.

Рисунок 1 – График зависимости эффективности предварительной обработки

Т.е. подходящее соотношение между стабильностью и количеством необходимых ФНФ ячеек должно быть найдено в зависимости от применения.

Идея подхода преселекции аналогична подходам, известным из биометрической техники: только значимые характеристики данных используются для идентификации или в процессе аутентификации. Во время преселекции только характерные ячейки ФНФ выбираются для обеспечения данных для выхода ФНФ. Характерные ячейки, это те ячейки, которые с небольшой вероятностью производят ошибки. Ячейки ФНФ меняют свои выходные значения при влиянии шума, температуры, старения, и других факторов окружающей среды. Ячейки, изменившие свои выходные данные, скорее всего, изменят их снова. Ячейки, которые изменяют выходной сигнал по любой причине, называются нестабильными. Ячейки ФНФ, которые всегда формируют ожидаемый результат, называются стабильными.. Цель состоит в том, что бы найти устойчивые ячейки уже на начальном этапе. Концепция показана на рисунке 2. В этом примере 100 ячеек ФНФ помещают в массив. Нестабильные ячейки зачеркнуты. Порядок маркировки стабильных ячеек называется преселекцией. Остальные 89 ячеек отбирают для дальнейшего пользования. В примере, эффективность e = 89%, После процесса преселекции частота ошибок должна уменьшаться.

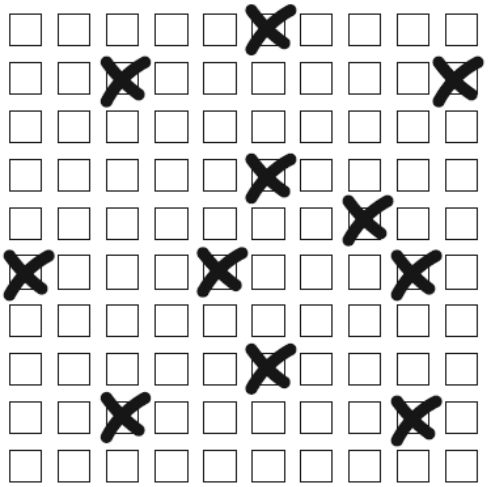

Рисунок 2 – Концепция преселекции

Существуют различные подходы для нахождения нестабильных ФНФ ячеек. В рамках первого подхода все клетки считываются несколько раз. Т.о. могут быть обнаружены ошибки, возникающие из-за шума. Во втором подходе, называемом преселекция пороговой обработки, выбираются только ячейки ФНФ с предопределенным минимальным несоответствием. Подход, который называется преселекция измерения времени, использует сумму времени, которое необходимо для решения ячеек. В преселек-

ции добавления заряда битовая очередь общих ячеек ФНФ предзаряжается для поиска нестабильных ФНФ ячеек.

1. Преселекция на основе многоразового чтения

В данном подходе измеряется выходные значения с ячеек ФНФ несколько раз. Те ячейки, которые всегда обеспечивают тот же результат, помечаются как полезные. Ячейки, которые не всегда обеспечивают тот же результат, не используются больше. Программное обеспечение должно контролировать процесс считывания на начальном этапе. Информация должна храниться в энергонезависимой памяти. На первый взгляд это кажется хорошим подходом, но на практике возникают различные проблемы. Имеется много циклов считывания, для нахождения ячеек, которые имеют низкую вероятность ошибки. Другие проблемы возникают из-за различных условий окружающей среды. Такие ошибки оказываются хуже, чем ошибки, произведенные шумом, для большинства типов ФНФ. Например, некоторые ячейки ФНФ изменяют свои выходные значения при перегреве. Проблема изображена на рисунке 3. Первоначальная оценка делается при температуре +25 ◦C (рисунок 3а). После некоторых считываний, семь ячеек ФНФ изменяют свое выходное значение и поэтому они помечены как нестабильные. Если температура падает до -40 ◦C, различные ячейки ФНФ нестабильны, чем при +25 ◦C. Только три из нестабильных ячеек ФНФ изменяют свое поведение при обеих температурах (рисунок 3б). Аналогичная ситуация и при +120 ◦C. Некоторые из ячеек ФНФ не устойчивы, но только единицы из этих ячеек неустойчивы при +25 ◦C.

Рисунок 4а показывает зависимость частоты появления битовых ошибок от температуры в одной точке преселекции на основе многоразового чтения. Максимальная частота ошибок не может быть многократно снижена. Что бы решить эту проблему, начальные измерения должны быть сделаны во всем диапазоне температур,

Если выполняется начальное считывание, как описано выше, результат показан на рисунке 4б. Используя данный подход преселекции, частота появления битовых ошибок может резко снизиться. К сожалению, считывание при различных температурах в течении начального этапа дорого и не может считаться реалистичной процедурой, что бы уменьшить частоту появления ошибок.

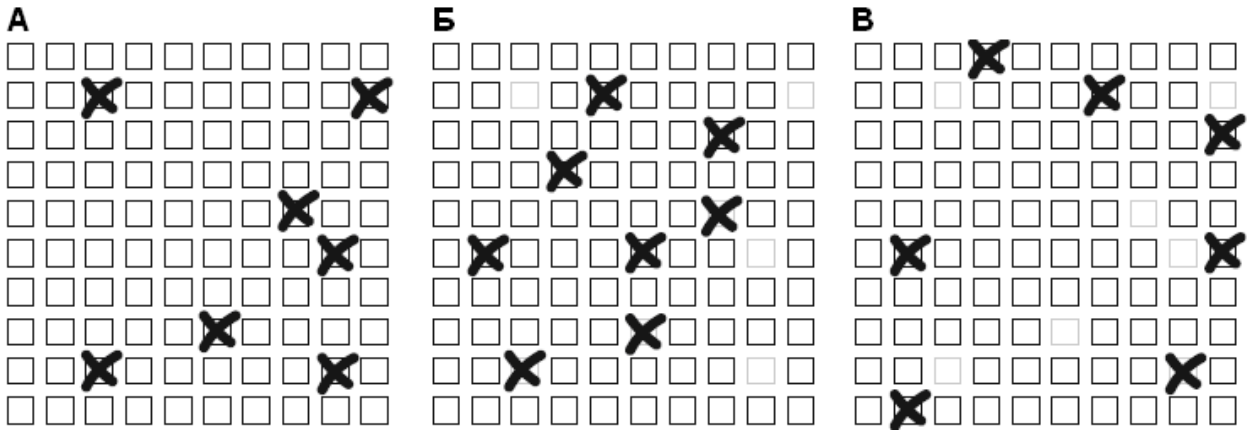

Рисунок 3 (а) Нестабильные ячейки ФНФ при +25 ◦C; (б) Нестабильные ячейки ФНФ при –40◦C; (в) Нестабильные ячейки ФНФ при +120 ◦C

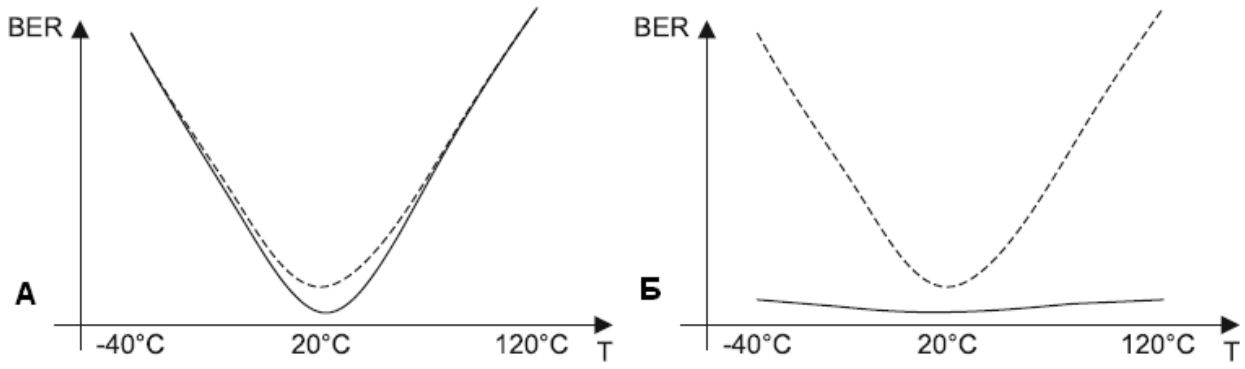

Рисунок 4 – Частота появления ошибочных битов (BER) в зависимости от температуры до (пунктирная линия) и после преселекции на основе многоразового чтения (сплошная линия) (а) При температуре +20 ◦C; (б) При трех температурах (–40◦C, 20◦C, 120◦C)

Другим решением данной проблемы может стать искусственное увеличение шума в ячейках. При таком подходе менее неустойчивые ячейки также могут быть обнаружены во время нескольких считываний при комнатной температуре. Для этого необходим генератор шума.

2. Преселекция пороговой обработки

Второй подход, основан на выборе ячеек, которые обеспечивают несоответствие, которое превышает определенный порог.

Например, в случае с ФНФ на основе СОЗУ это несоответствие между вовлеченными транзисторами, которое должно быть больше, чем заданное пороговое значение. Рисунок 5 показывает пороговое напряжение несоответствие (ΔVth) схематично распределенных пар транзисторов. Две пунктирные линии показывают заданный положительный (ΔVth+) и отрицательные (ΔVth–) пороговые значения, где |ΔVth+| = |ΔVth–|. Пороговое значение разделяется функцией распределения в трех областях: центральная площадь включает в себя все пары, чьи несоответствия слишком малы. Они отмечены как неполезные (NUF). Области слева и справа включают все пары, чьи несоответствия превышают пороговое значение. Эти пары обозначены либо UF+ (положительное несоответствие), либо UF- (отрицательное несоответствие).

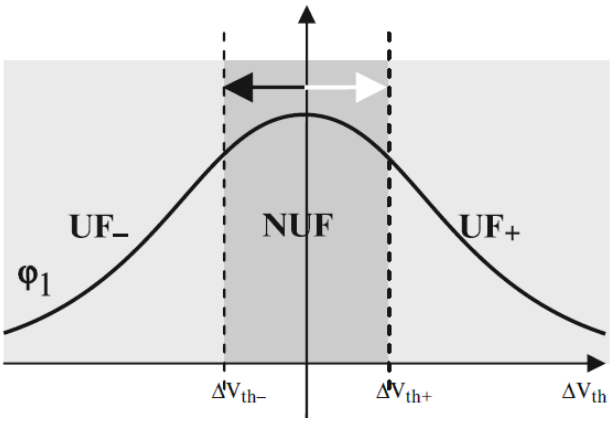

Рисунок 5 – Несоответствие разделено на три группы: Полезные ФНФ ячейки с положительным несоответствием (UF+), полезные ФНФ ячейки с отрицательным несоответствием (UF-) и неполезные ФНФ ячейки (NUF)

Что бы обеспечить стабильный выход ФНФ, порог должен быть выбран правильно, что бы получить ожидаемый уровень ошибок. Выбор порогового значения является компромиссом между частотой появления ошибок и количеством требуемых ячеек ФНФ. Если пороговое значение выбрано большим, то частота ошибок получается невысокой, но количество неиспользуемых пар получается большим. И наоборот: если пороговое значение выбрано маленьким, то количество выбранных пар и частота ошибок будет большим.

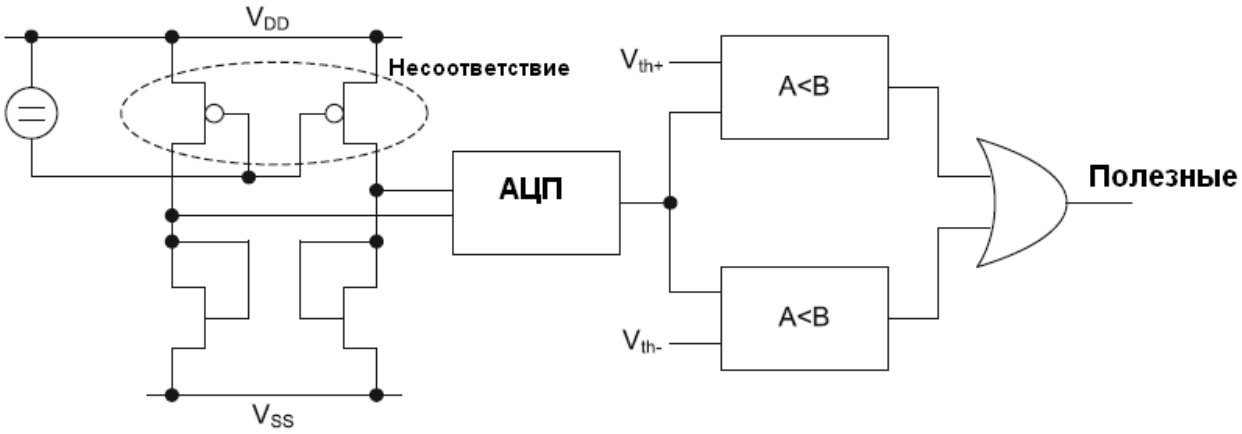

Рисунок 6 – Измерение несоответствия, используя АЦП

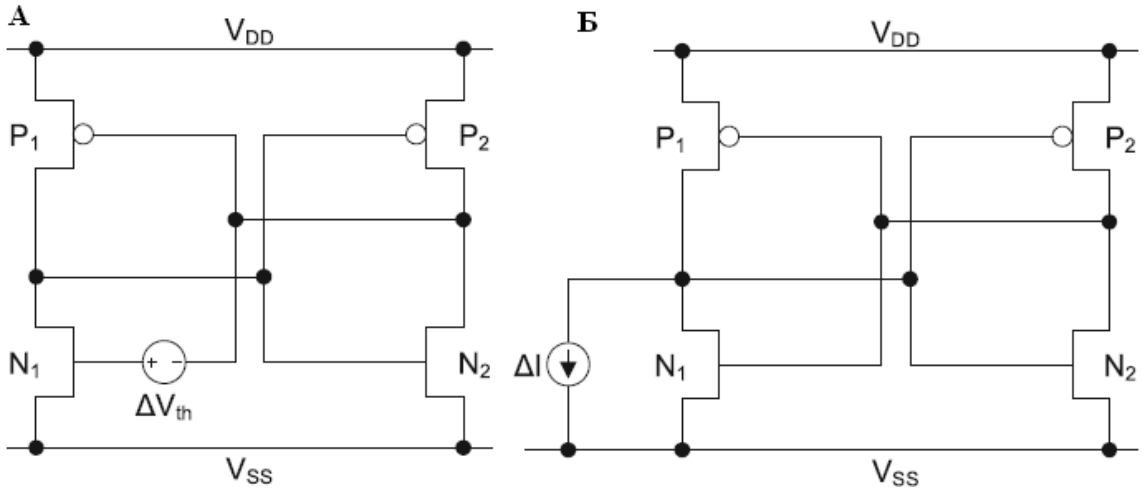

Рисунок 7 – (а) ячейка СОЗУ с дополнительным источником напряжения на затворе N1; (б) ячейка СОЗУ с дополнительным источником тока на стоке N1

Одним из способов найти неустойчивые ячейки, заключается в измерении несоответствия ΔVTth, используя общий аналогово-цифровой преобразователь (АЦП). На рисунке 6 изображена блок-схема такого подхода. Здесь, несоответствующие компоненты это два транзистора. Из-за несоответствия напряжение на транзисторах отличается. Эта разница напряжений измеряется на АЦП. Ячейка выбирается, если разница превышает порог.

К сожалению, есть некоторые недостатки, связанные с АЦП подходом. Т.к. АЦП будет добавлять как можно меньшее смещение измерения, то АЦП должно быть большого размер. Кроме того, АЦП не должен зависеть от шума в цепи для предотвращения ошибок. Однако, разрешающая возможность АЦП может быть маленькой.

Еще один подход заключается в добавлении искусственного несоответствия во время измерений. Здесь необходимы по крайне мере два измерения, что бы обнаружить является ли ячейка полезной или нет. При первом измерении добавляется отрицательное смещение. Т.о. пороговое значение равно Vth–. При

втором измерении, порог перемещается в Vth+. Это показано на рисунке 5 двумя стрелками. Если несоответствие транзисторов превышает порог, то ячейки ФНФ будут предоставлять такое же выходное значение при обоих измерениях. Если несоответствие мало, то выходные значения будут отличаться при измерениях.

Данный подход преселекции может быть реализован различными способами. Схема, реализована с использованием обычных СОЗУ ячеек, изображена на рисунке 7. Транзисторы P1 и P2 разработаны таким образом, что они были согласованы. Т.о., несоответствие между двумя n-МОП транзисторами N1 и N2 определяют поведение при подаче питания. Для реализации преселекции источник дополнительного напряжения должен быть подведен к одному n-МОП транзистору. Этот источник напряжения позже обеспечивает смещение преселекции (рисунок 7а). Вместо реализации источника напряжения на затворе, его эквивалент, источник тока, должен быть введен параллельно одному из n-МОП транзисторов (рисунок 7б). Т.к. два транзистора имеют разные Vth, количество тока, проходящего через транзисторы, отличается при одинаковом напряжении затвор-исток (Vgs). Т.о. дополнительное протекание через параллель одного из транзисторов эквивалентно разнице Vth.

3. Преселекция измерения времени

Одной из возможностей для измерения стабильности ячеек ФНФ это измерение времени до достижения ячейки определенного выходного напряжения. СОЗУ ячейка (рисунок 8) имеет следующие преимущества: она мала, состоит только из 6 транзисторов, включенных в транзисторную линию, и простая функциональность. Идея подхода заключается в том, что стабильным ФНФ ячейкам нужно меньше времени для определяющего процесса, чем нестабильным ячейкам.

Причиной такого поведения является несоответствие порогового напряжения между вовлеченными транзисторами. Для упрощения анализа предполагается, что МОП транзисторы хорошо согласуются. Т.о., решение зависит только от двух n-МОП транзисторов. Кроме того предполагается, что источники ошибок, такие как шум, старение и температурные сдвиги, непосредственно влияют на пороговое напряжение и т.о. они имеют влияние на выходной сигнал. Если питание включено, напряжение на узлах A и B лежит где-то между Vdd и Vss, в зависимости от емкостей затворов вовлеченных транзисторов. Если пороговое напряжение транзистора N2 меньше, чем Vth на N1, то ток, протекающий через правую ветвь, будет больше чем ток, протекающий через левую ветвь. Т.о., напряжение на узле B ниже, чем напряжение на узле A. Если напряжение на узле B меньше, то напряжение Vgs на P1 выше, и напряжение на точке A увеличивается. Это положительная обратная связь. Чем выше различие между пороговыми напряжениями транзисторов, тем быстрее будет найдена стабильная точка. Т.о. схема обнаружения должна быть реализована для измерения времени, необходимого для принятия решения.

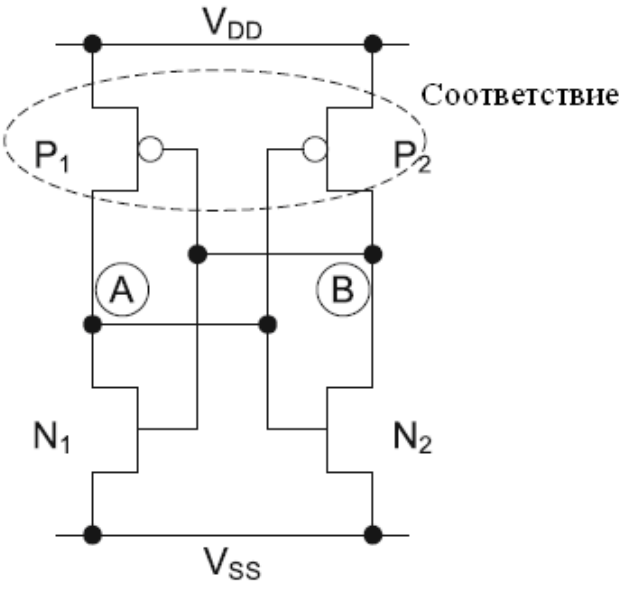

Рисунок 8 – Ячейка СОЗУ

На рисунке 9 показана концепция практической реализации. В левой части можно увидеть ячейки ФНФ. Схема измерения задержки изображена в правой части. Сигнал SEL активирует ячейки ФНФ. Два компаратора сравнивают выходное значение порогового напряжения на двух выходных узлах ячейки

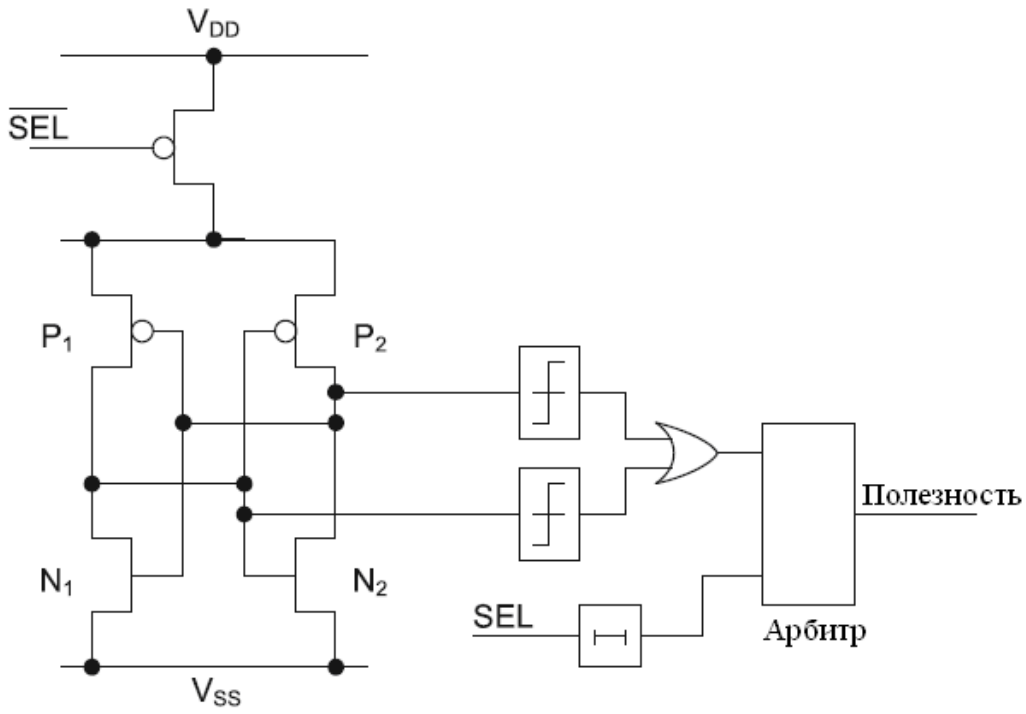

Рисунок 9 – Концепция преселекции с измерением времени

ФНФ. Необходимо только положительное пороговое напряжение. Желаемое выходное напряжение будет достигнуто через некоторое время на одном из двух компараторов. Два выхода компараторов объединяются с помощью логического элемента ИЛИ. Этот сигнал подается на арбитр. На другой вход арбитра подается задержанный сигнал SEL. SEL сигнал, который активируется ячейкой ФНФ, задерживается, используя соответствующую схему. Арбитр сравнивает два сигнала. Если задержанный SEL сигнал прибывает позже, чем выходное значение с компаратора, то на выходе арбитра будет 1. В этом случае, ФНФ определяется полезной.

4. Преселекция добавления заряда

В дополнении к уже описанным подходам, ФНФ ячейки могут быть смещены, используя заряды, которые вводится в схему по удобным узлам. Эти заряды вводятся в процессе принятия решения и помогают в поиске тех ячеек, которые имеют небольшое несоответствие, которое вероятно будет производить ошибки в будущем.

Принятие решения ФНФ СОЗУ зависит от несоответствия между различными транзисторами. Несоответствий напряжений Vth двух p-МОП транзисторов в большей степени определяют выходное значение ячеек. В случае небольшого несоответствия между этими p-МОП, а также n-МОП N1, N2 и различные емкости транзисторов могут влиять на выходное значение. Для нахождения ячеек с небольшим несоответствием каждую ячейку считывают один раз со смещенной левой ветвью и один раз со смещенной правой ветвью. Если ячейка возвращает такое же значение для обоих случаев, то ячейка рассматривается как стабильная. Степень смещения определяется количеством стабильных ФНФ ячеек.

Для смещения СОЗУ ячеек схема смещения должна иметь доступ к отдельным ветвям ячейки. Смещение на ветвях ФНФ СОЗУ может быть, в основном, сделано через все выводы СОЗУ: Vss, Vdd, WL, BL. Vss, Vdd, WL не могут управляться отдельно в оригинальной схеме. Что бы иметь возможность использовать эти выводы по отдельности для преселекции – схема должна быть модифицирована.

Только напряжение на BL может управляться отдельно для двух различных ветвей с большим преимуществом, т.к. СОЗУ оптимизировано в плане размера. Следовательно, нужно использовать схемы без какой-либо модификации.

Важно, что бы все схемы начинались со значения Vb = 0 для обеих ветвей. Это может быть сделано путем сброса всех узлов включением ФНФ СОЗУ. Способ смещения зависит от используемого вывода (Vss, Vdd, WL, BL).

4.1. Vss

Если Vss используется для смещения, то Vss одной из двух ветвей увеличиться. Уменьшение невозможно, т.к. исток/подложка диода может быть открыта. Если Vss возрастает, то Vgs уменьшается для этого транзистора и ток, протекающий через N1/N2, будет формировать задержку для этой ветви. На рисунке 10 изображена схема. Перед подачей напряжения на ячейку, Vss одной из ветвей увеличивается до заранее определенного значения. Подход не влияет на поведение p-МОП транзисторов, но влияет на поведение n-МОП транзисторов, и т.о. косвенно влияет на процесс принятия решения.

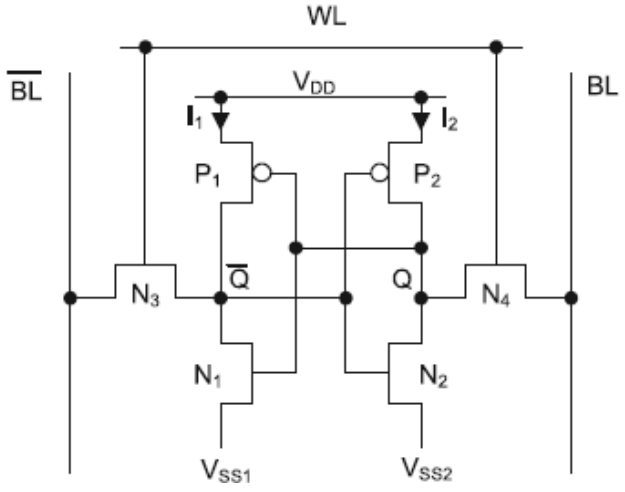

Рисунок 10 – Преселекция с использованием вывода Vss

4.2. Vdd

Если Vdd используется для смещения, то Vdd одной ветви увеличивается быстрее чем Vdd другой ветви. Это делается путем введения двух различных токов через узлы Vdd двух ветвей. Смещенная ветвь будет достигать Vth раньше, чем включение номинального напряжения и т.о, это будет влиять на принятие решения ячеек. Подача напряжения на схему – это динамический процесс, и становиться тяжело контролировать течение тока. Емкости включенных ФНФ ячеек будут отличаться, главным образом, для двух ветвей и они будут влиять на крутизну наклона Vdd. Рисунок 11 показывает схему.

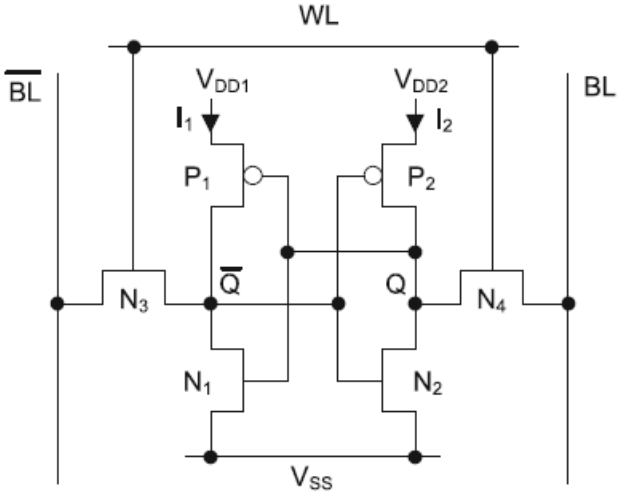

Рисунок 11 – Преселекция с использованием вывода Vdd

4.3. WL

Напряжение на выводе WL может быть использовано для производства смещения заряда на Q/Qn. Что бы это сделать, после сброса схемы, напряжение на одном из WL-транзисторов слегка возрастает. В связи с увеличением отверстий на затворе электрода, напряжение на Q/Qn увеличивается. В течении включения питания Vgs на p-МОП на несмещенной ветви уменьшается, и т.о. транзистор проводит ток позже чем при номинальном режиме. Это будет вынужденное принятие решение смещения точки к Vdd. Дополнительно, Vgs на n-МОП несмещенной точки возрастает, и принятие решение будет двигаться к

Vdd. Используя этот подход, важно убедиться, что Vth на WL-транзисторе не возрастает, т.к. это будет подключено к Vb на BL и это уничтожит функциональность ФНФ. Т.к. емкости между затвором и истоком/стоком малы, механизм предзаряда довольно нечувствителен к шуму на напряжении WL. На рисунке 12 изображена схема.

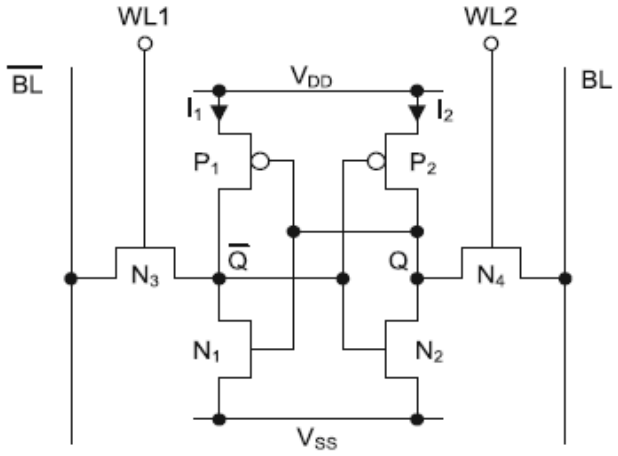

Рисунок 12 – Преселекция с использованием вывода WL

4.4. BL

BL выводы это только выводы, которые могут доступны по отдельности для двух различных ветвей. Это делает преселекцию с помощью BL очень привлекательной, т.к. схема не должна быть изменена. Как и в случае с WL-смещением, смещение использует битовую линию транзисторов и является основой для схемы с предварительным зарядом на Q/Qn. Смещение происходит путем изменения напряжения на BL, которое так же влияет на напряжение на Q/Qn до тех пор, пока транзистор WL в настоящее время открыт. На рисунке 13 показана схема.

Т.к. битовая линия BL является единственным соединением, которая разделена между двумя линиями СОЗУ, использование BL является наиболее привлекательным подходом преселекции ячеек СОЗУ.

В отличии от других подходов, выпадающее значение частоты ошибок будет существовать за счет шума. Это делает важным использование мажоритарного решения при многоразовом запуске в дополнении к преселекции для того что бы свести к минимуму влияние выпадающих значений шума.

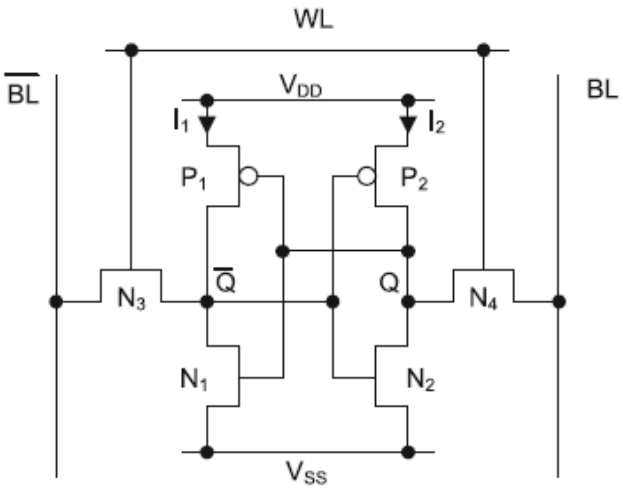

Рисунок 13 – Преселекция с использованием вывода BL

Выводы

После преселекции на основе многократного считывания, частота появления битовых ошибок по-прежнему остается слишком высокой. Тем не менее, этот вид преселекции может быть хорошим подходом для сокращения частоты битовых обишок таким образом, что бы обеспечить небольшую сложность коррекции ошибки для постобработки выходных данных. Кроме того, этот подход преселекции может быть совмещен с одним из других подходов преселекции, в будущем, для уменьшения частоты ошибки.

При преселекции пороговой обработки частота ошибок может быть снижена до 10^{E-12}. В связи с сильным снижением частоты ошибок последующая обработка может быть реализована менее сложной или даже становится ненужной. Кроме того, меньший коэффициент ошибок позволяет снизить энергопотребление и более увеличивает скорость считывания. Дополнительное усиление, вызываемое процессом преселекции, мало по сравнению с преимуществом, т.к. каждый элемент считывается только дважды во время инициализации. Кроме того, инициализация может быть сделана при одной температуре.

Список литературы

1. Ярмолик В.Н., Вашинко Ю.Г. Физически неклонируемые функции // Информатика. 2011. №2. – С.92 – 103.
2. Суханов С.В. Сравнительный анализ конструкций кремниевых физически неклонируемых функций / Суханов С.В., Коваленко М.П., Игнатенко И.А// Известия Института инженерной физики. 2014. №2(32). – С.2–6.
3. Bohm C., Hofer M. Physical Unclonable Functions in Theory and Practice. – NY.: Sprynger, 2013. – 270 p.
4. Hofer M., Boehm C. An alternative to error correction for sram-like pufs // workshop on cryptographic hardware and embedded systems. 2010. – 335-350 p.