Инженерный вестник Дона, №3 (2015)
ivdon.ru/ru/magazine/archive/n3y2015/3167

Влияние напряжения питания на характеристики физически неклонируемых функций арбитрового типа

А.Ю. Лосевской

АО «НИИМЭ», Зеленоград

Аннотация: Представлены результаты экспериментального исследования влияния напряжения питания на характеристики физически неклонируемых функций (ФНФ) арбитрового типа. Исследуемые образцы ФНФ были реализованы в процессе уровня 0,18 мкм ОАО «НИИМЭ и Микрон». В ходе исследования было обнаружено негативное влияние систематических вариаций на уникальность ФНФ. Снижение напряжения питания до уровня порогового напряжения позволяет повысить уникальность ФНФ. Кроме того, результаты эксперимента показывают, что надежность ФНФ сильно зависит от точности источника напряжения питания цепочек ФНФ.
Ключевые слова: интегральная схема, идентификация, физически неклонируемая функция, арбитр, Arbiter PUF.

Введение

Неизбежные неконтролируемые технологические вариации процесса производства ИС делают каждую ИС уникальной на молекулярном уровне. У топологически идентичных ИС электрофизические параметры пассивных и активных элементов слегка отличаются друг от друга. Так, например, несовершенство процесса фотолитографии приводит к вариациям длины и ширины затвора транзисторов, несовершенство процесса имплантации вызывает вариацию концентрации примеси в канале и пр. [1].

Физически неклонируемая функция [2-5] реализуется в виде функционального блока, встраиваемого в ИС, который позволяет представить уникальность физической структуры ИС в виде бинарной последовательности. Данные последовательности могут быть использованы в качестве идентификаторов ИС и криптографических ключей. Кроме того, на основе таких последовательностей могут быть построены протоколы аутентификации, позволяющие защитить ИС от копирования.

В данной статье изложены результаты исследования влияния напряжения питания на характеристики ФНФ арбитрового типа. Тестовые

образцы ФНФ были реализованы в КМОП процессе уровня 0,18 мкм ОАО «НИИМЭ и Микрон».

ФНФ арбитрового типа

В основе ФНФ арбитрового типа лежит цепочка сдвоенных мультиплексоров (рис.1).

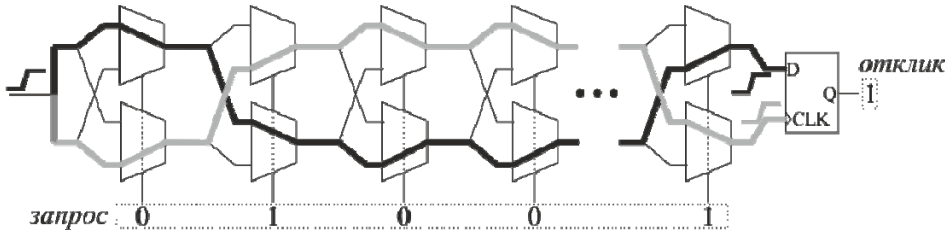

Рис. 1. – Конструкция ФНФ арбитрового типа

Сдвоенные мультиплексоры позволяют формировать пары симметричных путей, форма которых определяется бинарной последовательностью (запросом) на управляющих выводах мультиплексоров. Несмотря на то, что пути топологически симметричны, неизбежные технологические вариации процесса производства ИС приводят к тому, что задержка сигнала на этих путях будет слегка отличаться. На конце цепочки размещается арбитр, который позволяет представить в бинарной форме соотношение задержек на путях (отклик). В качестве арбитра могут выступать D-триггер или RS-защелка [6]. Каждому запросу соответствует отклик, уникальный для каждой ИС.

Для получения отклика на вход цепочки подается сигнал с положительным фронтом, который в начале цепочки раздваивается. Сигналы распространяются по двум симметричным путям, обретают, вследствие технологических вариаций, разные задержки и, наконец, защелкиваются арбитром.

На основе откликов могут быть сформированы бинарные последовательности произвольной длины, для этого можно использовать, например, генератор псевдослучайных чисел, где в качестве затравки используется запрос.

Характеристики ФНФ арбитрового типа

Основными характеристиками ФНФ арбитрового типа являются внутричиповая уникальность, межчиповая уникальность и надежность.

Для численной оценки характеристик используется понятие расстояния Хэмминга (HD) для двух последовательностей. HD подсчитывает число битовых позиций, в которых последовательности отличаются. Так, например, для последовательностей «00110010» и «10100101» HD равно 5 бит.

Внутричиповая уникальность показывает, насколько в среднем отличаются бинарные последовательности одной и той же ФНФ, полученные при использовании разных запросов. Межчиповая уникальность показывает величину отличия бинарных последовательностей разных ФНФ для одного и того же запроса. В идеальном случае, когда присутствуют только случайные вариации, среднее значение расстояния HD для внутричиповой и межчиповой уникальности должно составлять половину длины последовательности. На практике негативное влияние на уникальность могут оказать систематические вариации, вызывающие перекосы в цепочке ФНФ.

Надежность указывает на устойчивость бинарных последовательностей ФНФ по отношению к различным факторам, таким как изменение напряжения питания, температуры и старение. В идеальном случае бинарные последовательности всегда должны быть устойчивыми. В реальности значения некоторых битов последовательности могут изменяться под влиянием вышеперечисленных факторов.

В данной работе изложены результаты экспериментального исследования влияния напряжения питания на уникальность и надежность ФНФ.

Тестовый кристалл ФНФ

Тестовый кристалл для исследования характеристик ФНФ арбитрового типа был изготовлен в КМОП процессе уровня 0,18 мкм ОАО «НИИМЭ и Микрон».

В кристалле было размещено 16 цепочек ФНФ с количеством стадий равным 64. Каждая стадия представляет собой два мультиплексора из набора стандартных ячеек, управляющие выводы которых объединены. Чтобы обеспечить топологическую симметрию путей цепочки мультиплексоры были размещены в смежных строках. В качестве арбитра был использован RS-триггер на основе двух логических элементов «2И-НЕ» с перекрестной обратной связью, которые также были размещены в смежных строках. Цепочки ФНФ принадлежат отдельному домену питания, что позволяет проводить исследование зависимости характеристик ФНФ от напряжения питания. Для согласования уровней сигналов между доменами питания цепочек и управляющей логики использовались схемы сдвига уровней.

Для формирования бинарных последовательностей длиной 128 бит был использован 64-битный генератор псевдослучайных чисел, при этом запрос являлся затравкой для генерации 128-ми внутренних запросов, непосредственно подаваемых на цепочку.

Для исключения внутрисхемных шумов, неизбежно возникающих в процессе сбора данных, каждая последовательность генерировалась 11 раз, и далее, в процессе обработки данных, использовалось ее усредненное значение.

Всего было исследовано 8 тестовых кристаллов. Напряжение питания цепочек ФНФ (V_{PUF}) в процессе сбора бинарных последовательностей

варьировалось в диапазоне от 0,45 до 2,00 В с шагом 0,05 В, температура окружающей среды была равной +25 °С.

Далее по тексту принято следующее обозначение образцов: Ф*N*-*K*, где *N* – номер кристалла (от 1 до 8), *K* – порядковый номер ФНФ в кристалле *N* (от 1 до 16).

Внутричиповая уникальность

В ходе анализа экспериментальных данных было обнаружено, что у большей части образцов имеется заметная зависимость внутричиповой уникальности от напряжения питания V_{PUF} (рис.2). На рис.3 представлены гистограммы распределения образцов по внутричиповой уникальности при пониженном, номинальном и повышенном напряжениях V_{PUF}. Из данного рисунка следует, что снижение напряжения питания цепочек позволяет улучшить внутричиповую уникальность для большинства образцов.

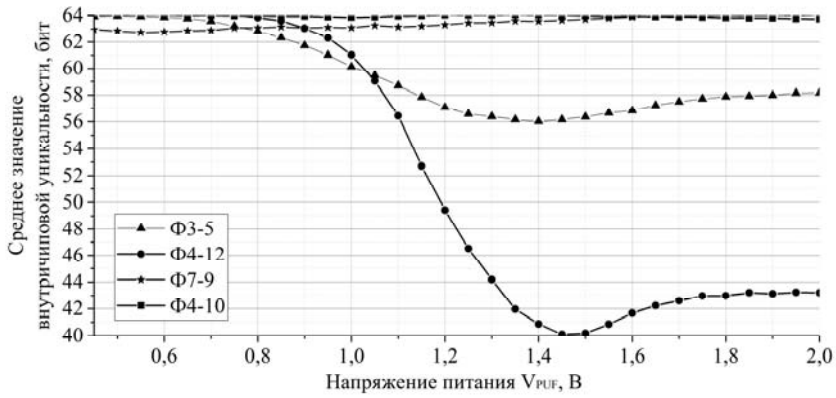

Рис. 2. – Влияние напряжения питания V_{PUF} на внутричиповую уникальность

Представленное разнообразие зависимостей (рис.2) может быть объяснено различной степенью влияния разных технологических вариаций на задержку элементов цепочки, при этом сама степень влияния вариаций зависит от напряжения питания. Среди технологических вариаций, имеющих наибольшее влияние на задержки, можно выделить вариацию длины затвора

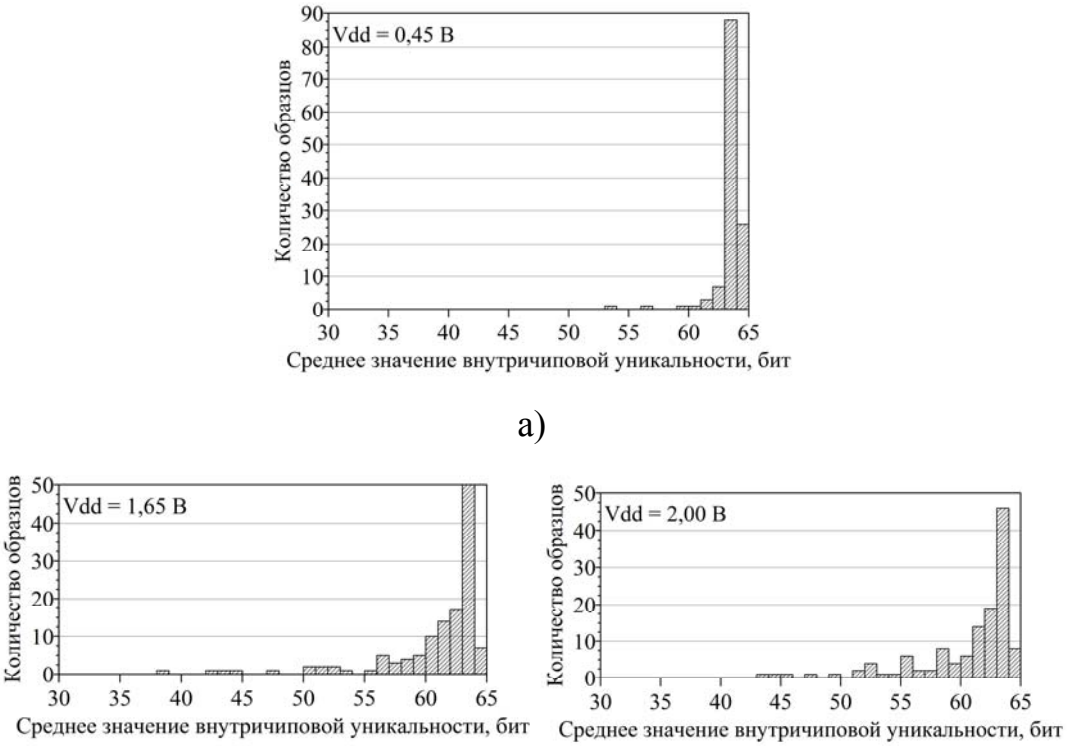

Рис. 3. – Распределение образцов по внутричиповой уникальности при пониженном (а), номинальном (б) и повышенном (в) напряжениях питания

и вариацию порогового напряжения транзисторов. При снижении напряжения питания до уровня порогового зависимость тока транзистора от порогового напряжения приобретает экспоненциальный характер, что приводит к преобладанию влияния вариаций порогового напряжения над вариациями длины затвора. Присутствие систематической вариаций может привести к снижению уникальности, если при данном напряжении питания систематическая вариация имеет наибольшее влияние на задержку (см. зависимость корреляционных коэффициентов задержки от напряжения питания для разных типов вариаций в работе [7], стр. 18).

Для примера рассмотрим зависимости для некоторых образцов (рис.2). Образец Ф4-10 имеет уникальность, которая практически не зависит от напряжения питания, что говорит об отсутствии сколько-нибудь значимых

систематических вариаций. Однако исследование надежности данного образца показало, что для одних и тех же запросов последовательности, полученные в области низких напряжений, отличаются от последовательностей, полученных при высоких напряжениях, в среднем на 40%. Данное наблюдение позволяет сделать вывод, что в области низких напряжений преобладают случайные вариации порогового напряжения, тогда как в области высоких напряжений – случайные вариации длины затвора. У образца Ф4-12 в области высоких напряжений начинают проявляться систематические вариации длины затвора, тогда как в области низких напряжений преобладают случайные вариации порогового напряжения. Образец Ф7-9 в области пониженных напряжений имеет небольшое снижение уникальности вследствие проявления систематических вариаций порогового напряжения, при этом в области высоких напряжений преобладают случайные вариации длины затвора.

Низкая внутричиповая уникальность ФНФ приводит к снижению межчиповой уникальности и в конечном итоге к негативному росту значений вероятности ложного отказа (FRR) и вероятности ложного совпадения (FAR) [8] в системах идентификации. Кроме того, снижается устойчивость ФНФ к построению математического клона с использованием методов машинного обучения [9].

Исходя из всего вышесказанного, можно сделать вывод о необходимости снижения напряжения питания цепочек ФНФ до уровня пороговых напряжений для улучшения внутричиповой уникальности.

Надежность

Для оценки надежности сравнивались последовательности, полученные при некотором значении референсного напряжения питания V_{PUFREF}, с последовательностями, полученными при варьировании напряжения питания

V_{PUF} в диапазоне от 0,45 до 2,00 В с шагом 0,05 В. В идеальном случае число неустойчивых бит должно быть равно 0.

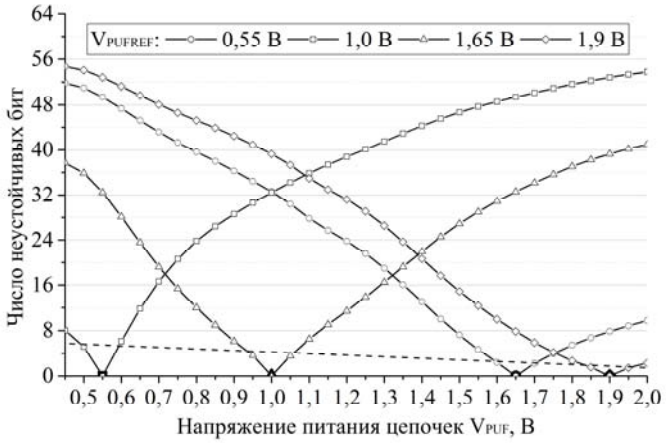

Рис. 4. – Зависимость надежности от напряжения V_{PUF} для разных значений V_{PUFREF} (усреднение по всем образцам)

На рис.4 представлены зависимости надежности (числа неустойчивых бит) от напряжения V_{PUF} для некоторых значений V_{PUFREF}. Как видно из рисунка наблюдается увеличение числа неустойчивых бит в последовательностях с понижением V_{PUFREF}. Предполагается, что данная зависимость вызвана ростом влияния вариаций порогового напряжения на задержки цепочек ФНФ при снижении напряжения V_{PUFREF}.

Надежность, как и внутричиповая уникальность влияет на устойчивость к построению математического клона и на идентификационные возможности ФНФ. Таким образом, точность источника напряжения питания цепочек ФНФ является важным фактором, влияющим на надежность ФНФ [10].

Межчиповая уникальность

Для оценки межчиповой уникальности производилось сравнение бинарных

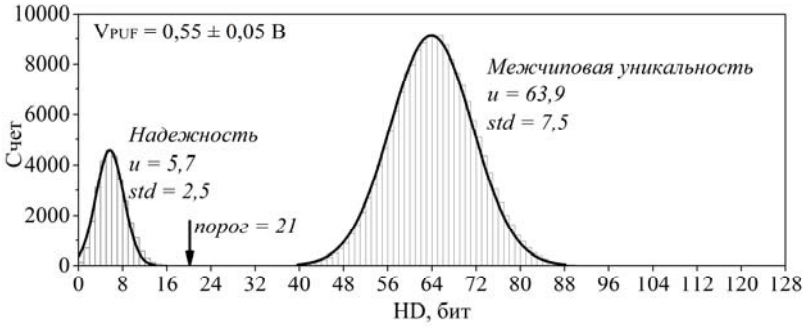

Рис. 5. – Межчиповая уникальность и надежность ФНФ

последовательностей разных ИС. Как и ожидалось, улучшение внутричиповой уникальности с понижением напряжения V_{PUF} приводит к улучшению межчиповой уникальности. На рис.5 представлены гистограммы межчиповой уникальности и надежности для случая отклонения напряжения V_{PUF} на 0,05 В от референсного значения 0,55 В. Как видно из рисунка среднее значение HD для межчиповой уникальности составляет величину близкую к идеальной (половина длины последовательности, т.е. 64 бита). Кроме того, данный рисунок позволяет оценить идентификационные возможности ФНФ. Так, например, для успешной идентификации группы ИС, порог может быть установлен равным 21-му биту, при этом значения FRR и FAR имеют порядок 10^{-9}.

Заключение

ФНФ позволяют сформировать для каждой ИС набор бинарных последовательностей, которые могут быть использованы для идентификации и защиты ИС от копирования.

Результаты исследования экспериментальных образцов указывают на необходимость использования точных источников напряжения питания цепочек, поскольку даже небольшие отклонения напряжения от расчетного значения приводят к заметному снижению надежности, что негативно влияет на идентификационные возможности ФНФ.

Выявленные систематические вариации негативно влияют на уникальность ФНФ. Снижение напряжения питания до уровня порогового напряжения позволяет повысить уникальность за счет преобладающего влияния случайных вариаций порогового напряжения.

В дальнейшей работе планируется изучить влияние температуры окружающей среды и эффекта старения ИС на характеристики ФНФ.

Литература

1. Красников Г. Я., Конструктивно-технологические особенности субмикронных МОП-транзисторов. В 2 ч.. М.: Техносфера, 2004. 416 с. и 536 с.

2. 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 // Международная научно-практическая конференция «Научные исследования и их практическое применение. Современное состояние и пути развития ‘2012». Одесса: Куприенко СВ, 2012. С. 23-38.

3. Tajik, S., E. Dietz and S. Frohmann, 2014. Physical Characterization of Arbiter PUFs. Cryptographic Hardware and Embedded Systems – CHES 2014, Springer Berlin Heidelberg, pp: pp 493-509.

4. Edward Suh, G., 2007. Physical unclonable functions for device authentication and secret key generation. Design Automation Conference, ACM, pp: 9-14.

5. Majzoobi, M., F. Koushanfar and M. Potkonjak, 2008. Lightweight secure PUFs. ICCAD '08 Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design, IEEE Press Piscataway, pp: 670-673.

6. Ермаков И.В., Шелепин Н.А. Схемотехнические решения R-S- и D-триггеров с электрически перепрограммируемой энергонезависимой памятью

// Инженерный вестник Дона, 2014, №2 URL: ivdon.ru/ru/magazine/archive/n2y2014/2453.

7. Low Voltage Circuit Design Techniques for Cubic Millimeter computing. URL: michigancmes.org/papers/scott_hanson_thesis_2009.pdf.

8. Hospodar, G., 2012. Machine Learning Attacks on 65nm Arbiter PUFs: Accurate Modeling poses strict Bounds on Usability. Information Forensics and Security (WIFS), IEEE, pp: 37-42.

9. Devadas, S., 2010. Modeling Attacks on Physical Unclonable Functions. Computer and communications security, ACM, pp: 237-249.

10. Бормонтов Е.Н., Сухотерин Е.В., Колесников Д.В., Невежин Е.В. Чувствительность КМОП-источника опорного напряжения к вариациям параметров элементов // Инженерный вестник Дона, 2014, №1 URL: ivdon.ru/ru/magazine/archive/n1y2014/2275.

References

1. Krasnikov G. Ya., Konstruktivno-tekhnologicheskie osobennosti submikronnykh MOP-tranzistorov [Constructive and technological features of submicron MOSFETs]. V 2 ch.. M.: Tekhnosfera, 2004. 416 p. i 536 p.

2. Losevskoy A.Y. Mezhdunarodnaya nauchno-prakticheskaya konferentsiya «Nauchnye issledovaniya i ikh prakticheskoe primenenie. Sovremennoe sostoyanie i puti razvitiya ‘2012». Odessa: Kuprienko SV, 2012. pp. 23-38.

3. Tajik, S., E. Dietz and S. Frohmann, 2014. Physical Characterization of Arbiter PUFs. Cryptographic Hardware and Embedded Systems – CHES 2014, Springer Berlin Heidelberg, pp: pp 493-509.

4. Edward Suh, G., 2007. Physical unclonable functions for device authentication and secret key generation. Design Automation Conference, ACM, pp: 9-14.

5. Majzoobi, M., F. Koushanfar and M. Potkonjak, 2008. Lightweight secure PUFs. ICCAD '08 Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design, IEEE Press Piscataway, pp: 670-673.

6. Ermakov I.V., Shelepin N.A.Inženernyj vestnik Dona (Rus), 2014, №2 URL: ivdon.ru/ru/magazine/archive/n2y2014/2453.

7. Low Voltage Circuit Design Techniques for Cubic Millimeter computing. URL: michigancmes.org/papers/scott_hanson_thesis_2009.pdf.

8. Hospodar, G., 2012. Machine Learning Attacks on 65nm Arbiter PUFs: Accurate Modeling poses strict Bounds on Usability. Information Forensics and Security (WIFS), IEEE, pp: 37-42.

9. Devadas, S., 2010. Modeling Attacks on Physical Unclonable Functions. Computer and communications security, ACM, pp: 237-249.

10. Bormontov E.N., Sukhoterin E.V., Kolesnikov D.V., Nevezhin E.V. Inženernyj vestnik Dona (Rus), 2014, №1 URL: ivdon.ru/ru/magazine/archive/n1y2014/2275.