УДК 621.3.082.74

Выявление контрафакта внутри однородной партии микросхем при измерении s-параметров

А.В. Семенов, В.Н. Федорец

ФГУП 18 ЦНИИ МО РФ, antony.se@yandex.ru

***Аннотация* — Задача подтверждения однородности микросхем важна для выявления бракованных и контрафактных изделий в партии. В данной работе сделана попытка упрощения анализа микросхем за счет использования их s-параметров для оценки однородности партии. Это особенно актуально в связи с быстро возрастающим количеством контрафактной продукции.**

***Ключевые слова* — контрафакт, NBTI, HCI, s-параметры.**

I. Введение

В современных условиях ужесточившейся проблемы контрафакта задача быстрого выявления таких микросхем становится чрезвычайно важной. Оценивание характеристик микросхем должно занимать минимальное время и учитывать наиболее опасные классы контрафактных микросхем. Изучение выявленных контрафактных изделий в мире за последние годы позволило сформировать ряд стандартов в области защиты потребителей от контрафактных микросхем [1-3]. Описанный в этих стандартах подход к выявлению контрафакта учитывает идентификационные признаки микросхем, обладающие наибольшей общностью, так как смещение фокуса на отдельные группы схем значительно увеличивает стоимость и время проведения испытаний. Результаты [4] проведенных к настоящему времени исследований показали, что свойства основных классов контрафакта можно описать в базисе качества: надежность, функциональность, энергопотребление, стоимость, производительность. При этом различные классы контрафакта влияют на различные измерения принятого базиса качества.

Основные, наиболее опасные классы контрафакта находятся в работоспособном состоянии и приведены в «товарный» вид для продажи. Это микросхемы, не прошедшие испытания производителя по отдельным параметрам, несанкционированные клоны оригинальных микросхем и, так называемые, восстановленные изделия, выработавшие большую часть ресурса. Для учета влияния старения на параметры микросхем используются модели эффектов деградации параметров. Целью настоящей работы является построение методики выявления контрафактных микросхем на основе измерения *нестандартных* аналоговых параметров.

II. Существующие методы

Выявление контрафакта с помощью известных методов визуального контроля и акустической микроскопии не позволяют выявлять качественно перемаркированный контрафакт.

Существующие инструменты экспресс-анализа, например, с помощью сравнения ВАХ [1,5], не всегда способны выявлять дефекты контрафактных микросхем, связанные со старением, так как чувствительность метода ограничена. Метод оценивания надежностных характеристик микросхем и блоков радиоэлектронной аппаратуры с помощью низкочастотного шума [6] при неоспоримых достоинствах обладает избыточной точностью. Отдельные методы характеризации микросхем с целью выявления неоднородностей базируются на весьма подробных моделях вентильного уровня [7, 8], что не всегда удобно и доступно при исследовании микросхем, с которыми не поставляются подробные модели. В то же время активно используемые методы анализа цифровых схем на поведенческом уровне трудоемки для схем с большим количеством выводов и не позволяют выявлять такой обширный класс контрафакта, как восстановленные изделия [9].

Задача подтверждения однородности партии микросхем (выявления неоднородности) в общем случае сводится к анализу нескольких образцов и отсеиванию тех, которые выходят за установленные интервалы допустимых параметров. При анализе микросхем различные неразрушающие методы анализа обладают различной чувствительностью, что приводит к пропуску неоднородных изделий или к необходимости проведения дополнительных испытаний.

Микросхемы внутри партии в условиях единого технологического процесса могут различаться из-за различных факторов. Первая группа факторов обусловлена технологической изменчивостью, помеховыми эффектами, типовыми неисправностями. Вторая группа факторов обусловлена неправильным комплектованием партии или наличием в партии контрафактных микросхем. Авторы предполагают, что мера отличия большинства классов контрафактных микросхем, приведенных во введении, будет превышать меру отличия в рамках технологической изменчивости между микросхемами (что отчасти подтверждено исследованиями [10]).

Анализ партий микросхем для выявления контрафакта должен проходить максимально оперативно с целью минимизации задержки выпуска продукции.

Мы предлагаем альтернативный подход выявления неоднородных микросхем в партии на основе анализа широко известных s-параметров.

Таким образом, содержательная постановка задачи сводится к выбору такой измеримой модели микросхемы, которая позволила бы в условиях ограниченного времени проводить экспресс-анализ партии однотипных микросхем для анализа однородности партии с целью выявления контрафактных микросхем или неправильно укомплектованных партий.

III. Базовые модели различия контрафактных микросхем

С учетом анализа результатов по зафиксированным инцидентам с контрафактом [11] рассматриваются модели двух наиболее опасных классов контрафакта: восстановленные изделия, а также контрафакт, имитирующий реальные изделия, основанный на краже интеллектуальной собственности.

A. Восстановленные микросхемы

Первая модель - восстановленный контрафакт, характеризуется необратимыми изменениями в структуре, что приводит к дрейфу отдельных электрических и временных параметров [10]. Для данного типа микросхем характерно комплектование контрафактной партии из различных источников, что приводит к отличиям в версиях («степпинге») микросхем, геометрической конфигурации кристалла в корпусе и т.п. Отдельные признаки такого контрафакта могут быть выявлены с помощью визуального контроля, рентгеновской или акустической микроскопии, однако качество подделок растет. Параметрическая модель восстановления характеризуется следующими влияющими процессами:

1) NBTI (Negative-bias temperature instability) – температурная нестабильность напряжения обратного смещения [12].

2) HCI (Hot Carrier Injection) – инжекция горячих носителей [12].

Оба процесса приводят к необратимому изменению пороговых напряжений транзисторов. Формулы для расчета приведены в [12].

3) TDDB (Time-dependent dielectric breakdown) – пробой диэлектрика, зависящий от времени [13].

Обозначим изменения задержки прохождения сигналов, вызванных отдельными эффектами как ΔD_{NBTI}, ΔD_{HCI}, ΔD_{TDDB}. Общее изменение задержки сигнала, вызванной деградацией параметров, обозначим как $\Delta D_{\deg}$.

B. Имитация оригинала с сохранением функций

Рассмотрим вторую модель контрафакта, характеризующую ситуацию кражи интеллектуальной собственности, когда базовые функции схемы сохраняются, но с изменением внутренней структуры/процесса.

Предположим, что граф G, описывающий исходную схему, изоморфен графу G', описывающему контрафактную схему. В условиях различия количества вершин и веса ребер на основе алгоритмов анализа межсоединений [14] изменится задержка прохождения сигнала ΔD_{ISO}, то есть импульсный отклик четырехполюсника, который через преобразование Фурье однозначно связан с АЧХ (s_{11}).

Кроме этого, на различия микросхем влияют внутри- и междусхемные вариации процесса изготовления. Совокупное влияние технологической изменчивости на задержку распространения сигнала обозначим как $\Delta D_{PV} = \Delta D_{внутрPV} + \Delta D_{межсхPV}$.

IV. Используемые метрики оценки RC-цепей

В качестве базовой модели представления микросхемы используется сеть межсоединений [15]. Эта модель в отношении микросхем использует физические характеристики сопротивлений, индуктивностей и емкостей. Таким образом, базовой структурой для расчета становится так называемая RLC модель, базирующаяся на эквивалентных преобразованиях электрических цепей для расчета основных параметров схемы.

Пользуясь терминологией теории графов можно представить связи между входом и выходом устройства как сеть межсоединений с ребрами, имеющими характер линейного преобразования и вершинами, обозначающими некоторое нелинейное преобразование.

Рассматривая отдельные методы статистического временного анализа [14, 15], которые позволяют рассчитать помеху, влияющую на время прохождения сигнала, для каждой цепи в качестве базовой гипотезы было решено выбрать возникновение помехи задержки [14], обусловленной первой или второй моделями контрафакта. В этом случае может меняться порядок функционирования узлов агрессоров (для модели один) или изменяться значение максимально реализуемого набора узлов агрессоров (для модели два). В простейшем случае отличия, обусловленные контрафактным характером микросхем, могут быть смоделированы в виде дополнительного паразитного эффекта [16], изменяющего свойства сети межсоединений. Сопутствующие шумы [6] учитываются с помощью повторения измерений.

V. Предлагаемые модели измерения

Анализ различных моделей полупроводниковых устройств показал [16], что модели на основе s-параметров позволяют моделировать работу сложных устройств без излишней детализации и используются в более сложных моделях анализа работы микросхем, например в области электромагнитной совместимости (ICEM, PDN [17], Feature Selective Validation Method [16]) или целостности сигналов (IBIS модели [16]).

Использование s-параметров, как наиболее информативных при измерении паразитных эффектов сетей межсоединений, основано на предположении, что модификация сети межсоединений в терминах исполь-

зуемых метрик распространения сигнала при измерении в одинаковых условиях приведёт к достоверным результатам.

Во временной области сформируется интервал для заданного пути прохождения сигнала от ΔD_{med} до ΔD_{PV}, где ΔD_{med} - среднее изменение задержки синхросигнала для нескольких измерений, ΔD_{PV} – оценка изменения задержки, обусловленной технологической изменчивостью.

Наша гипотеза заключается в том, что для приведенных моделей контрафакта $\Delta D_{\deg}$ и ΔD_{iso} находятся за границами этого интервала, что подтверждается отдельными научными результатами [18], и при переходе в частотную область позволяет использовать s-параметры для оценки большого частотного диапазона, при условии проведения всего лишь одного измерения для одного пути прохождения сигнала (рис. 1).

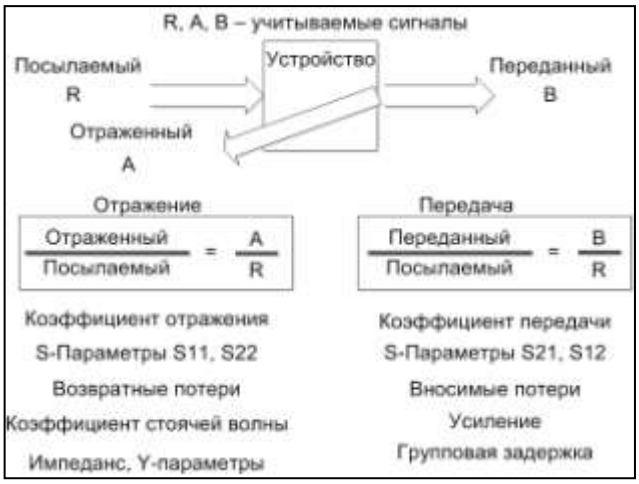

Рис. 1. Общая схема работы и основные параметры векторного анализа цепей

Выбранный подход первоначально основан на сравнении характеристик случайных процессов на выходе устройства без оглядки на конкретные внутренние состояния анализируемой системы, что позволяет пренебречь сложными нелинейными связями внутри микросхем.

Необходимо отметить, что измерение s-параметров (векторный анализ) подразумевает низкоэнергетическое воздействие на объект исследования, что позволяет избежать нежелательных побочных эффектов при испытаниях.

VI. Методика контроля однородности партии

Текущий метод проверки однородности построен на предположении, что все измерения производятся при одинаковой температуре и окружающих условиях.

Ниже перечислены этапы методики.

1) Построение эталонного совместного распределения.

Проведем n измерений s-параметров для эталонного прибора из партии на заданном диапазоне частот от f_1 до f_2, причем каждое измерение производится между двумя различными выводами микросхемы.

2) Получение совместного распределения измеренных значений векторов.

По центральной предельной теореме в случае с s-параметрами примем гипотезу о нормальности распределений.

3) Построение ковариационной матрицы.

Представляя измерения в виде многомерной случайной величины, с учетом, что элементы м.с.в. в нашем случае имеют конечные дисперсии, построим ковариационную матрицу $\Sigma = (\sigma_{ij})$, $i,j=1,\ldots,n$, в которой элементы $\sigma_{ij} = \operatorname{cov}(X_i, X_j) = E(X_i - EX_i)\ (X_j - EX_j)$ - ковариации случайных величин X_i, X_j. На главной диагонали находятся дисперсии DX_i случайных величин X_i.

Для оценивания ковариационной матрицы по многомерной выборке *A* используем стандартную формулу $\hat{\Sigma} = (m-1)^{-1} A^T A$.

4) Выяснить условную вероятность по сравнению с эталонными значениями.

Для определения вероятности события *J* – эталонного измерения требуется рассмотреть некоторое количество гипотез, соответствующих отдельным измерениям: $H_1, H_2, \ldots, H_n$, где *n*-количество измерений.

В случае, если гипотезы несовместные (микросхема контрафактная, микросхема новая), условная вероятность рассчитывается по формуле Байеса.

5) Рассчитать вероятность попадания в эллипс рассеивания.

Предполагая, что значения условных вероятностей распределены по нормальному закону, мы рассчитываем вероятность попадания в область рассеивания как $p = 1 - e^{-0,5}$.

6) Построить доверительный интервал, в котором достоверны результаты.

При доверительной вероятности β=90% доверительный интервал для дисперсии вычисляется по формуле $I_\beta = (\tilde{m} - \varepsilon_\beta; \tilde{m} + \varepsilon_\beta)$, где $\varepsilon_\beta = t_\beta \sqrt{\frac{\tilde{D}}{n}}$.

Отметим, что верхняя и нижняя границы доверительного интервала, полученные с помощью центральной предельной теоремы, носят асимптотический характер и их точность повышается с ростом выборки.

VII. Результаты

Описанный алгоритм предлагается для измерения партий микросхем. При этом для моделирования клонированных функций применялся логический синтез

логической схемы на ПЛИС, выполненной по технологии 65 нм, с 12 слоями металла (медь). Предварительные измерения s-параметров показали фиксируемые различия эталонной схемы и модифицированного варианта с формированием в частотной области (см. рис. 2, 3).

На основе предлагаемых в данной работе методик проектируется программно-аппаратный комплекс исследования партий микросхем с целью выявления контрафакта.

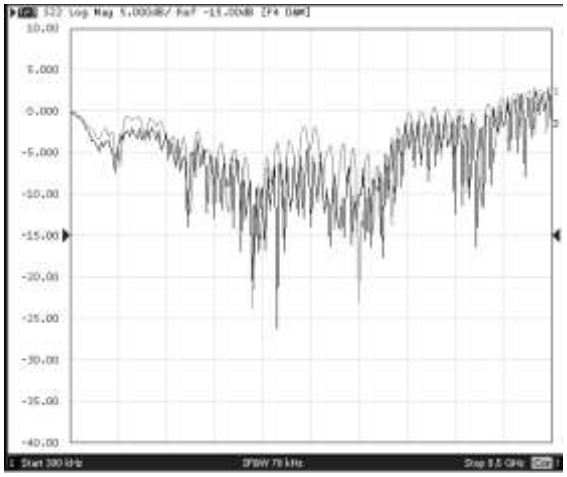

Рис. 2. Отличие s-параметров между выводами микросхемы при анализе исходного графа (серый цвет) и изоморфного графа (черный цвет)

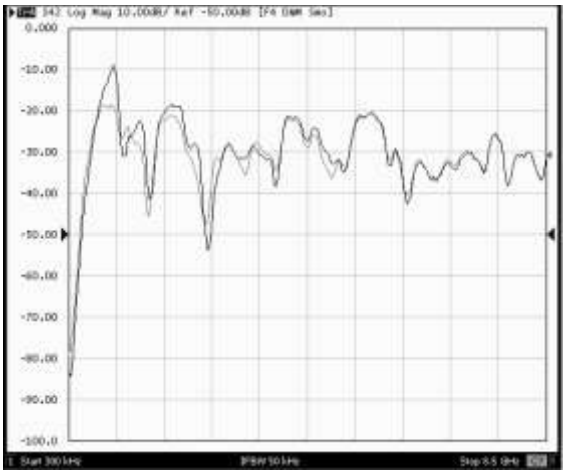

Рис. 3. Отличие s-параметров между выводами микросхемы при анализе исходного графа (серый цвет) и изоморфного графа (черный цвет) в режиме сглаживания

Благодарности

Благодарим Потапова А.Ю. за помощь в проведении измерений.

Литература

[1] SAE, Counterfeit electronic parts; avoidance, detection, mitigation, and disposition, 2009, http://standards.sae.org/as5553/. [20.12.13].

[2] CTI, Certification for coutnerfeit components avoidance program, Sept. 2011, http://www.cti-us.com/pdf/CCAP101Certification.pdf. [20.12.13].

[3] IDEA, Acceptability of electronic components distributed in the open market, http://www.idofea.org/products/118-idea-std-1010b. [20.12.13].

[4] Белов Е.Н., Захаренков А.И., Пономарев А.А., Семенов А.В., Федорец В.Н. Информационная безопасность в микроэлектронике: защита отечественных производителей от контрафактной продукции // 12-я НТК Твердотельная электроника. Сложные функциональные блоки РЭА. Москва, 2013.

[5] Sentry ABI Counterfeit detector. http://abielectronics.co.uk/Products/SENTRYCounterfeitICDetector.php/. [20.12.13].

[6] Жигальский П.Г. Флуктуации и шумы в электронных твердотельных приборах. М.: ФИЗМАТЛИТ. 2012. 512 с.

[7] Liu B. Gate Level Statistical Simulation Based on Parameterized Models for Process and Signal Variations // Quality Electronic Design, 2007. ISQED '07. 8th International Symposium. 26-28 March 2007. P. 257,262. doi: 10.1109/ISQED.2007.84.

[8] Alkabani Y. et al. Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach / In Information Hiding, Kaushal Solanki, Kenneth Sullivan, and Upamanyu Madhow (Eds.) // Lecture Notes In Computer Science. Vol. 5284. Springer-Verlag, Berlin, Heidelberg 102-117. DOI=10.1007/978-3-540-88961-8_8 http://dx.doi.org/10.1007/978-3-540-88961-8_8

[9] Roy J.A., Koushanfar F., Markov I.L. (2008) EPIC: Ending Piracy of Integrated Circuits // Proc. on Design, Automation and Test in Europe: 1069-1074.

[10] Zhang X., Xiao K., Tehranipoor M. Path-delay fingerprinting for identification of recovered ICs // Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium. 3-5 Oct. 2012. P. 13,18. doi: 10.1109/DFT.2012.6378192.

[11] U.S. Department Of Commerce (2010) Defense Industrial Base Assessment: Counterfeit Electronics.

[12] Wang Y., Cotofana S., Fang L. A unified aging model of NBTI and HCI degradation towards lifetime reliability management for nanoscale MOSFET circuits // Nanoscale Architectures (NANOARCH), 2011 IEEE/ACM International Symposium. 8-9 June 2011. P. 175,180. doi: 10.1109/NANOARCH.2011.5941501.

[13] Choudhury M., Chandra V., Mohanram K., Aitken R. Analytical model for TDDB-based performance degradation in combinational logic // Design, Automation & Test in Europe Conference & Exhibition (DATE) 2010. 8-12 March 2010. P. 423,428. doi:10.1109/DATE.2010.5457168.

[14] Стемпковский А.Л. Методы логического и логико-временного анализа цифровых КМОП СБИС / А.Л. Стемпковский, С.В. Гаврилов, А.Л. Глебов / под общ. ред. А.Л. Стемпковского. Ин-т проблем проектирования в микроэлектронике РАН. М.: Наука, 2007. 220 с. - ISBN 978-5-02-036119-5.

[15] Celik M., Pileggi L., Odabasioglu A., IC Interconnect Analysis. Springer. 2002. 310 с.

[16] Leventhal R., Green, L. Semiconductor Modeling:: For Simulating Signal, Power, and Electromagnetic Integrity. Springer. 2006. 768 с.

[17] Ben Dhia S., Ramdani M., Sicard E. Electromagnetic Compatibility of Integrated Circuits. Springer. 2006. 473 с.