УДК 621.3.082.74 DOI 10.31114/2078-7707-2018-4-143-148

Технометрическая идентификация микросхем для контроля жизненного цикла и поиска контрафакта

А.В. Семенов, В.Н. Старцев, Е.Н. Степанов

ФГУП 18 ЦНИИ МО РФ, г. Москва, ewgenij.stepanoff42@yandex.ru

***Аннотация* — Рассмотрена возможность контроля и идентификации микросхем и других изделий электронной техники. В частности, предложен подход идентификации, основанный на измерениях аналоговых характеристик изделия, рассматриваемого как "черный ящик". Для построения системы использован аппарат биометрии и физически неклонируемых функций. Мы получаем набор свойств, которыми должна обладать система идентификации, чтобы говорить о технометрии интегральных микросхем. Для предложенного подхода классические задачи биометрии могут быть переформулированы как: технометрический контроль (поиск контрафакта, сопоставление с эталоном один-к-одному) и идентификация (контроль на протяжении жизненного цикла – сопоставление один-ко-многим – подключение к базе данных для определения объекта после измерения технометрических данных). Показано, что измерения s-параметров позволяют идентифицировать микросхему и одновременно решать задачу идентификации и определения подлинных микросхем.**

***Ключевые слова* — контрафакт, идентификация интегральных микросхем, физически неклонируемые функции, биометрия.**

I. Введение

В современных условиях необходима идентификация применяемой в изделиях элементной базы. Особенно это важно при контроле изделий, предназначенных для работы в системах ответственного применения.

В целях выявления контрафактных микросхем желательна многофакторная идентификация, так как идентификаторы предусмотренные производителем микросхем, часто копируются или редактируются фальсификаторами [1]. Это касается, например, восстановленных микросхем, бывших в употреблении [2, 3]. При этом часть информации требуется хранить в секрете от потребителя для предупреждения подделки используемых идентификаторов. Таким образом, разработчики и производители интегральных микросхем пришли к введению многоуровневой идентификации для собственных нужд.

Решение близкой задачи маркировки микросхем для потребителя на протяжении всего жизненного цикла также сталкивается с определенными трудностями. Нанесение на микросхемы любого подобия акцизных марок (для считывания идентификационных признаков в видимом, инфракрасном и/или ультрафиолетовом диапазоне), использование радиочастотных меток, штриховых кодов сталкиваются с ограничениями условий использования микросхем. Разнообразие материалов корпусов, температурные ограничения – для подобных меток также важны, как стойкость к копированию и фальсификации. Голографические метки, скретч-панели и другие способы защищённой от подделки маркировки подходят в лучшем случае для маркировки тары и сопроводительной документации.

Системы маркировки можно условно разделить на информационные и защитные, которые, в свою очередь, могут быть открытыми или идентифицируемыми на экспертном уровне с помощью специального оборудования. Информационная метка – как правило заводская маркировка или этикетка, в лучшем случае обеспечивает первичные учетные потребности производителя, а не потребителя микросхем.

В данной работе рассматривается подход к созданию систем технометрической идентификации микросхем для решения двух разнонаправленных по математическому содержанию задач:

- идентификации на протяжении жизненного цикла в смысле использования уникальной сигнатуры или алгоритма распознавания, отличающего только набор характеристик, свойственных конкретной микросхеме;

- поиска контрафакта как задачи классификации исходных изделий на (по крайней мере) два класса – один из которых – класс подлинников, а другой – класс подозрительных на контрафакт; что требует от используемого алгоритма гораздо большей способности к обобщению, чем в первой задаче.

Предлагаемый подход позволил обобщить некоторые результаты из теории информации и теории машинного обучения для решения прикладной задачи сквозного контроля качества микросхем.

II. Известные результаты

Математическая постановка задачи поиска контрафакта, как правило, сводится исследователями к задаче кластеризации (если метки класса-подлинника отсутствуют) или классификации (если метки класса известны с достаточной долей вероятности). В качестве обучающих наборов выступают изображения – 2D, гиперспектральные, наборы измерений электрических

параметров или измерений, полученных с помощью физико-технического анализа [4].

Для обеспечения практического использования упомянутых подходов наиболее широко используются методы технического зрения и машинного обучения. При этом изображения внешнего вида дают весьма серьёзную погрешность даже при определении типовых дефектов [5]. Рентгеновская томография может приводить к снижению надежности памяти даже при ограниченной мощности источника излучения и суммарного времени экспозиции [6].

Кроме этого, встает вопрос о сложности обучения алгоритмов классификации, так как обобщающая способность обученных алгоритмов позволяет определять конкретные дефекты, распознавать маркировку, но не позволяет идентифицировать конкретную микросхему [6, 7].

Дополнительно, из практики проведения экспертизы микросхем на наличие признаков контрафактного исполнения известно: при испытании образцов, так или иначе, приходится использовать дополнительную маркировку в целях опознавания отдельных образцов в партии в процессе испытаний и учета в соответствующей базе данных. Требования к этой маркировке сходны по уровню с требованиями к самим микросхемам.

Таким образом, можно констатировать, что задача получения системы идентификации с одной стороны пригодной для опознавания микросхем на протяжении жизненного цикла, а с другой – позволяющая обнаруживать контрафактные микросхемы – на сегодняшний момент не решена окончательно.

В этой связи особый интерес представляет идентификация на основе некоторых естественных характеристик, причем такая, что вероятность коллизий при считывании характеристик сходных объектов в которой будет минимальна.

Для разрешения этой проблемной ситуации большинство разработчиков и производителей микросхем идут по пути внедрения идентификаторов в кристалл микросхемы [8]. В том числе основанных на использовании так называемых физически неклонируемых функций [9].

Производители микросхем только начинают промышленное использование данной технологии для идентификации собственной продукции, пока в контексте тех же специальных приложений безопасности и решения проблем генерации случайных чисел [10]. Физически неклонируемые функции позволяют извлекать характеристики объекта, зависящие от его физических свойств. При этом используется набор характеристик, достаточных для построения идентификации объекта, но не достаточный для решения обратной задачи.

В полупроводниковых устройствах используют технологическую изменчивость условий производства, основанную на параметрах конкретных структур [10, 11].

Идеальная ФНФ. Для имеющегося производственного процесса с имеющейся структурой объекта измерения идеальная ФНФ – это конструктивный элемент, который реализует функцию с областью определения, состоящей из запросов $C \subseteq \{0,1\}^{\lambda}$, и областью значений $R \subseteq \{0,1\}^{\eta}$, состоящих из откликов, где каждая функция зависит от изменений параметров производственного процесса и моделируется как случайный оракул. Для каждого запроса $c \in C$ имеющаяся функция возвращает определенный отклик r, который случайным образом равномерно выбирается из R и не зависит от изменения окружающих природных условий. Все значимые параметры заданы на интервалах напряжения $V \in [\alpha_V, \beta_V]$, температуры $T \in [\alpha_T, \beta_T]$ и максимальной продолжительности жизни определена β_L.

Подобный подход имеет определенные недостатки – в первую очередь – рост избыточности схемы.

В настоящий момент биометрические технологии все шире используются в нашей жизни [11, 12]. Их содержательным аналогом в технических системах являются ФНФ.

III. «Технометрическая» идентификация интегральных схем

A. *Общие требования*

Рассмотрим набор свойств, которым должна обладать система идентификации, чтобы можно было говорить о технометрии интегральных микросхем. По аналогии с биометрией [11] можно перечислить следующий набор характеристик:

1. Универсальность — каждый типовой объект должен обладать измеряемой характеристикой.
2. Уникальность — насколько хорошо один объект отделяется от другого с точки зрения используемого алгоритма различения.
3. Постоянство — мера того, в какой степени выбранные признаки остаются неизменными во времени, например в процессе эксплуатации.
4. Простота осуществления измерения.
5. Производительность — точность, скорость и надёжность используемой системы.
6. Приемлемость — степень достоверности работы системы.
7. Простота использования замены.

Тогда классические задачи биометрии примут следующий вид.

Технометрическая верификация (поиск контрафакта) — сравнение один к одному с шаблоном. Проверяет, что объект именно то, за что его выдают.

Технометрическая идентификация (контроль на протяжении жизненного цикла) — сравнение один ко многим: после «захвата» технометрических данных идет соединение с базой данных для определения объекта. Идентификация проходит успешно, если контрольные характеристики образца уже есть в базе данных.

Системой, наиболее близкой по свойствам к желаемой, являются ФНФ. Рассмотрим характеристику ФНФ, используемых в реальном мире.

Неидеальная ФНФ. Для имеющегося производственного процесса с имеющейся структурой объекта измерения неидеальная ФНФ – это конструктивный элемент, который реализует функцию с областью определения, состоящей из запросов $C \subseteq \{0,1\}^{\lambda}$, и областью значений $R \subseteq \{0,1\}^{\eta}$ состоящих из откликов, где распределение каждого случайного переменного R_i, $ci \in [1,|C|]$ зависит от технологической изменчивости, шума, переменных окружения и физической деградации параметров, вызванной старением.

Все значимые параметры заданы на интервалах напряжения $V \in [\alpha_V, \beta_V]$, температуры $T \in [\alpha_T, \beta_T]$ и максимальной продолжительности жизни β_L.

B. *Использование физической неклонируемости для технометрии*

Потребительские свойства технометрической системы идентификации, приведенные в предыдущем разделе, целесообразно рассматривать исходя из существующих подходов к определению качества ФНФ [12 – 15].

На основе анализа этих работ, определим следующий набор параметров, описывающих математические свойства ФНФ и требующих оценки перед проведением идентификации.

Для этого используем следующие обозначения.

$HD(r_i, r_j)$ – расстояние Хемминга между любыми двумя различными откликами r_i и r_j при одном и том же запросе;

N – количество микросхем/устройств в тестируемом наборе;

L – размерность отклика в битах;

K – количество ФНФ на одно устройство;

T – количество итераций считывания ФНФ.

$r_{n,mean}$ – средний отклик микросхемы n.

Тогда для оценки целесообразно использовать следующий набор параметров.

Uniformity – распределение 1 в откликах микросхемы n;

$$\frac{1}{KL}\sum_{k=1}^{K}\sum_{l=1}^{L} r_{n,k,l} \ . \quad (1)$$

BitAliasing – средние значения в бите l откликов различных микросхем;

$$\frac{1}{N}\sum_{n=1}^{N} r_{n,i} \ . \quad (2)$$

HD_{intra} - частота битовых ошибок в отклике $r_{n,t}$ микросхемы n на итерации t;

$$\frac{1}{TKL}\sum_{n=t}^{T} HD\left(r_{n,t}, r_{n,mean}\right)\times 100\% \ . \quad (3)$$

HD_{inter} - расстояний Хэмминга между откликами различных микросхем

В качестве иллюстрации и подтверждения возможности технометрии используем внутренний радиопортрет микросхем, удовлетворяющего базовым качествам идентификации.

IV. Экспериментальный анализ внутреннего радиопортрета для технометрии

Ранее мы предложили способ естественной идентификации радиотехнических изделий и микросхем как аналоговых, так и цифровых. Для этого используется набор радиочастотных характеристик, полученных с помощью векторного анализатора цепей, измеренных для конкретного изделия, в качестве его радиопортрета [16].

Радиопортрет на первый взгляд обладает универсальностью, уникальность, постоянством, простотой измерения и другими признаками, необходимыми технометрической системы.

Для фактического контроля важных характеристик рассчитаем значения свойств *Uniformity* (рис. 1), *BitAliasing* и HD_{inter} (рис. 2), HD_{intra} (рис. 3).

При этом методы расчета сходства на основе решения задачи кластеризации мы используем для контроля получаемых в математическом аппарате оценивания ФНФ интерпретации.

В качестве входных данных был использован обучающий набор [16].

Для преобразования исходных измеренных кривых радиопортрет был закодирован с помощью двоичного алфавита таким образом, что каждая точка на графике была преобразована в 6 битную строку. Конкатенация этих строк дала исходный идентификатор.

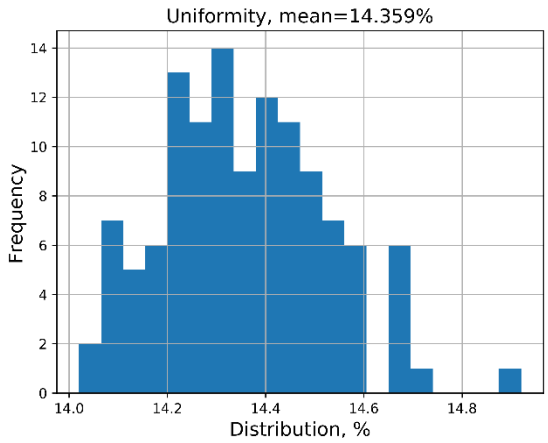

Рис. 1. Полученные характеристики *Uniformity*

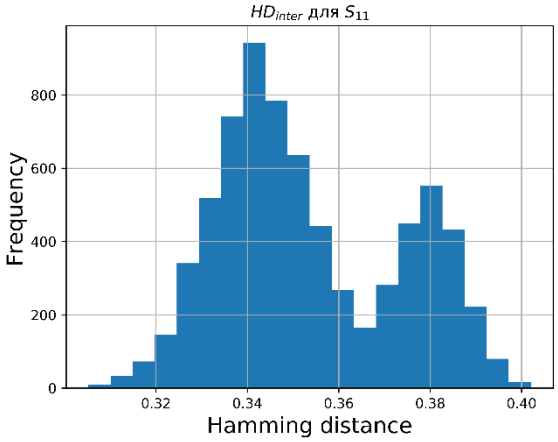

Рис. 2. Полученные характеристики HD_{inter}

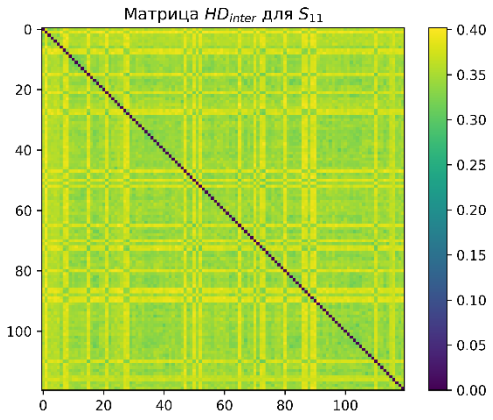

Рис. 3. Матрица расстояний HD_{inter} различных микросхем

Учитывая опорные характеристики показателей качества ФНФ для заданной частоты измерения, внутренний радиопортрет микросхемы является слабой ФНФ.

Для практического использования предлагается следующая схема технометрии.

Получение метки

1. Устройство, помеченное с s-меткой, проходит этап измерения для получения набора запрос-отклик в определенной полосе частот от f_1 до f_2.

2. С помощью схемы извлечения происходит перевод измерений в бинарную строку.

3. На основе предыдущих измерений происходит получение сигнатуры путем коррекции отклика для устранения возможных ошибок измерений.

4. Полученная строка сохраняется в базу.

Для других безчиповых меток данные этапы могут быть заменены применением расчетной модели.

Идентификация в класс подлинников или подделок

1. Устройство проходит этапы 1-3 из пункта «Получение метки»

2. Полученное значение разыскивается в базе данных. Если значение найдено – то устройство относится к классу подлинников, если нет – к классу подделок.

V. Обсуждение результатов

Очевидно, что применение технометрии не позволяет отказаться от дополнительных испытаний (как и получение биометрических данных ничего не говорит о здоровье человека). В то же время, однократное измерение для осуществления идентификации и верификации позволяет сэкономить время на проведение испытаний в ряде случаев.

Например, в описываемом примере исходное описание радиопортрета микросхемы может быть дополнено топологической информацией с указанием на то, между какими выводами он измерялся (для целей контроля собственных изделий).

VI. Выводы

Предложенная схема технометрической идентифкации интегральных микросхем решает сразу две задачи из области сквозного контроля качества интегральных микросхем.

В то же время очевидно, что наличие механизмов идентификации, стойкой к копированию и подделке являются маркетинговым преимуществом для производителей дорогостоящих микросхем.

Литература

[1] 2017 SITUATION REPORT ON COUNTERFEITING AND PIRACY IN THE EUROPEAN UNION URL: https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union (дата доступа: 27.11.2017 г.)

[2] Huang K. et al. Recycled IC detection based on statistical methods //IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2015. – Т. 34. – №. 6. – С. 947-960.

[3] Семенов А. В., Федорец В. Н. Выявление контрафакта внутри однородной партии микросхем при измерении s-

параметров //Проблемы разработки перспективных микро-и наноэлектронных систем (МЭС). – 2014. – №. 3. – С. 21-24.
[4] Лактионов А.В. и др. Выявление контрафактных электронных компонентов методами физико-технического анализа / А.В. Лактионов, И.В. Емельянова, Л.А. Ершов, А.В. Батурин, Р.Г. Левин, С. Э. Малютенкова // Петербургский журнал элек троники. – 2017. – № 2–3 (87)–(88) . – с. 29 – 44.
[5] Asadizanjani N. et al. A database for counterfeit electronics and automatic defect detection based on image processing and machine learning //ISTFA, Nov. – 2016.
[6] Dogan H. et al. Analyzing the Impact of X-ray Tomography on the Reliability of Integrated Circuits //Proc. 41st Int. Symp. Test. Failure Anal.(ISTFA). – 2015. – С. 1-10.
[7] Mahmood K. et al. Real-time automated counterfeit integrated circuit detection using x-ray microscopy //Applied Optics. – 2015. – Т. 54. – №. 13. – С. D25-D32.
[8] Peterson Ed. Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices // URL: https://www.xilinx.com/support/documentation/application_notes/xapp1323-zynq-usp-tamper-resistant-designs.pdf (Дата доступа: 03.02.2018 г.)
[9] Pappu, R. Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / R. Pappu // Massachusetts Institute of Technology (MIT). – Cambridge, 2001. – 154 p.
[10] Hori Y. et al. Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs // Reconfigurable Computing and FPGAs (ReConFig), 2010 International Conference on. – IEEE, 2010. – С. 298-303.
[11] Jain A. K., Ross A., Prabhakar S. An introduction to biometric recognition //IEEE Transactions on circuits and systems for video technology. – 2004. – Т. 14. – №. 1. – С. 4-20.
[12] Tuyls, P. Security with Noisy Data / P. Tuyls, B. Skoric, T. Kevenaar (ed.). – London :Springer, 2007. – 344 p.
[13] Maiti A. et al. A large scale characterization of RO-PUF //Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on. – IEEE, 2010. – С. 94-99.
[14] Su Y., Holleman J., Otis B. P. A digital 1.6 pJ/bit chip identification circuit using process variations //IEEE Journal of Solid-State Circuits. – 2008. – Т. 43. – №. 1. – С. 69-77.
[15] Maiti A., Gunreddy V., Schaumont P. A systematic method to evaluate and compare the performance of physical unclonable functions // Embedded systems design with FPGAs. – Springer New York, 2013. – С. 245-267.
[16] Семенов А. В., Федорец В. Н., Старцев В. Н. Контроль однородности партии типовых микросхем при измерении радиочастотных характеристик //Проблемы разработки перспективных микро-и наноэлектронных систем (МЭС). – 2016. – №. 3. – С. 49-56.

Technometric Identification of Integrated Circuits for Controlling Life Cycle and Counterfeit Detection

A.V. Semenov, V.N. Starcev, E.N. Stepanov

«18 central research institute», Moscow, ewgenij.stepanoff42@yandex.ru

***Abstract* — we considered the possibility of controlling and identifying chips and other electronic products. In particular, we propose an approach of identification based on measurements of analog characteristics of the product considered as a "black box". To build the system the instrument of biometrics and physically uncloneable functions is used. We get a set of properties those an identification system should possess, so we can talk about the technometry of integrated circuits. In relation to our approach, the classical biometric problem takes the following form: technometric verification (search for counterfeit, which means one-to-one comparison with the template) and identification (life cycle monitoring, which means one-to-many comparison, when after the "capture" of technometric data, a database connection is established to define the object). It has been shown on practice that the measurements of s-parameters allows identifying the chip and simultaneously solving the problem of identification and definition of authentic chips.**

***Keywords* — counterfeiting, identification of integrated circuits, physically uncloneable functions, biometrics.**

REFERENCES

[1] 2017 SITUATION REPORT ON COUNTERFEITING AND PIRACY IN THE EUROPEAN UNION URL: https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union (дата доступа: 27.11.2017 г.)
[2] Huang K. et al. Recycled IC detection based on statistical methods //IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2015. – Т. 34. – №. 6. – С. 947-960.
[3] Semenov A.V., Fedorets V. N. Detection of counterfeit inside a homogeneous batch of chips in the measurement of s-parameters / / problems of perspective micro-and nanoelectronic systems (MES). - 2014. - no. 3. - P. 21-24. (In Russian)
[4] Laktionov A. V. et al. Detection of counterfeit electronic components by methods of physico-technical analysis / A. V. Laktionov, I. V. Emelyanova, L. A. Ershov, V. A. Baturin, R. G., Levin, S. E. Malyenkov // St. Petersburg journal of electronic troniki. - 2017. – № 2-3 (87)–(88) . – p. 29 – 44. (In Russian)
[5] Asadizanjani N. et al. A database for counterfeit electronics and automatic defect detection based on image processing and machine learning //ISTFA, Nov. – 2016.
[6] Dogan H. et al. Analyzing the Impact of X-ray Tomography on the Reliability of Integrated Circuits //Proc. 41st Int. Symp. Test. Failure Anal.(ISTFA). – 2015. – С. 1-10.

[7] Mahmood K. et al. Real-time automated counterfeit integrated circuit detection using x-ray microscopy //Applied Optics. – 2015. – Т. 54. – №. 13. – С. D25-D32.
[8] Peterson Ed. Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices // URL: https://www.xilinx.com/support/documentation/application_notes/xapp1323-zynq-usp-tamper-resistant-designs.pdf (Дата доступа: 03.02.2018 г.)
[9] Pappu, R. Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / R. Pappu // Massachusetts Institute of Technology (MIT). – Cambridge, 2001. – 154 p.
[10] Hori Y. et al. Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs // Reconfigurable Computing and FPGAs (ReConFig), 2010 International Conference on. – IEEE, 2010. – С. 298-303.
[11] Jain A. K., Ross A., Prabhakar S. An introduction to biometric recognition //IEEE Transactions on circuits and systems for video technology. – 2004. – Т. 14. – №. 1. – С. 4-20.
[12] Tuyls, P. Security with Noisy Data / P. Tuyls, B. Skoric, T. Kevenaar (ed.). – London :Springer, 2007. – 344 p.
[13] Maiti A. et al. A large scale characterization of RO-PUF //Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on. – IEEE, 2010. – С. 94-99.
[14] Su Y., Holleman J., Otis B. P. A digital 1.6 pJ/bit chip identification circuit using process variations //IEEE Journal of Solid-State Circuits. – 2008. – Т. 43. – №. 1. – С. 69-77.
[15] Maiti A., Gunreddy V., Schaumont P. A systematic method to evaluate and compare the performance of physical unclonable functions // Embedded systems design with FPGAs. – Springer New York, 2013. – С. 245-267.
[16] Semenov A.V., Fedorets V. N., Startsev V. N. Control of the homogeneity of the batch of typical chips in the measurement of radio frequency characteristics / / problems of development of advanced micro-and nanoelectronic systems (MES). - 2016. - no. 3. – P. 49-56.(In Russian)