РАДИОСЕНСОРНАЯ ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ РАДИОЭЛЕКТРОННЫХ УСТРОЙСТВ

DOI: 10.36724/2072-8735-2022-16-5-15-20

Manuscript received 20 April 2022;
Accepted 11 May 2022

Бойков Константин Анатольевич,
МИРЭА – Российский технологический университет, Москва, Россия, ***nauchnyi@yandex.ru***

Ключевые слова: *сигнальный радиопрофиль, критерий Пирсона, частотно-временное преобразование, радиосенсорная идентификация, корреляционный анализ, декомпозиция*

Современные методы защиты радиоэлектронных изделий от незаконного клонирования имеют ряд серьезных недостатков, связанных с повышенным энергопотреблением, использованием процессорного времени, необходимостью гальванического доступа к объекту исследования. Частично указанные проблемы устраняют физически неклонируемые функции (ФНФ), позволяющие провести аутентификацию радиоэлектронного устройства. Однако и такого рода защита имеет серьезные уязвимости при незаконном перепроизводстве изделий сверх заказанного количества. К тому же ФНФ не позволяют провести идентификацию радиоэлектронных изделий. Целью данной работы является повышение защиты радиоэлектронных устройств от незаконного клонирования, путем исследования новой ФНФ, связанной с собственными электромагнитными излучениями радиоэлектронного устройства. В работе используются методы экспериментальных исследований для регистрации электрической составляющей излученного изделием электромагнитного поля – сигнального радиопрофиля (СРП). Методы корреляционного анализа для аутентификации изделия, статистический метод согласия Пирсона для идентификации. Представлены зарегистрированные от специально разработанных экспериментальных образцов СРП, проведен корреляционный анализ данных СРП. Для декомпозиции и экстракции параметров СРП построен его частотно-временной спектр. Составлена таблица соответствия и проведен анализ согласия Пирсона. Полученные результаты показали возможность использования СРП как новой физически неклонируемой функции, позволяющей провести идентификацию радиоэлектронных устройств с заданной исследователем вероятностью, что обуславливает новизну работы. Установлено, что при коэффициенте согласия Пирсона между параметрами исследуемого СРП и репера более 0,95 радиоэлектронное устройство может быть достоверно идентифицировано. Практическая значимость работы заключается в возможности использования СРП для идентификации группы устройств и радиотехнической защиты радиоэлектронного изделия от подделок и незаконных копий.

Информация об авторе:
Бойков Константин Анатольевич, *кандидат технических наук, доцент кафедры радиоволновых процессов и технологий Института радиоэлектроники и информатики ФГБОУ ВО "МИРЭА – Российский технологический университет", Москва, Россия*

Для цитирования:
Бойков К.А. Радиосенсорная идентификация и аутентификация радиоэлектронных устройств // T-Comm: Телекоммуникации и транспорт. 2022. Том 16. №5. С. 15-20.

For citation:
Boikov K.A. (2022). Radiosensor identification and authentication of radio-electronic devices. *T-Comm*, vol. 16, no.5, pp. 15-20. (*in Russian*)

Введение

Появление новых наукоемких решений на рынке радиоэлектронной индустрии для производителей оригинальной радиоэлектронной продукции зачастую сопровождается серьезными интеллектуально-правовыми и экономическими убытками. Это происходит в результате возрастающего числа подделок – контрафактных изделий. Современные методы защиты радиоэлектронных устройств (РЭУ) от нелегального клонирования и обратного проектирования – реинжиниринга (аппаратное шифрование, хеширование, внедрение цифровых водяных знаков) помогают решить данную проблему лишь частично, поскольку недостатками большинства перечисленных защитных мер являются значительные аппаратные затраты и, как следствие, высокое энергопотребление [1]. Такой подход противоречит современным требованиям к минимизации площади, занимаемой устройством на кристалле интегральной схемы, быстродействию и энергосбережению.

Одним из альтернативных способов аутентификации РЭУ являются ФНФ, которые значительно экономичны в реализации чем перечисленные выше методы защиты [2]. ФНФ основаны на использовании технологического разброса параметров интегральных схем – значений пороговых и опорных напряжений, задержек распространения сигналов, частотного диапазона функционирования отдельных компонентов. Отклонения параметров (технологическая изменчивость), присущие любому технологическому процессу и вызывающие соответствующие вариации формируемых физических структур, сравнительно недавно используются для обеспечения безопасности интегральных микросхем, для их аутентификации и генерации разного рода криптографических ключей [3]. Эти ФНФ напрямую используют некоторое производственные особенности схемы.

ФНФ являются аппаратным аналогом реализации хеш-функций, с отличием в выходном значении, основанном на уникальности конкретной интегральной схемы (либо компонента), а не на математическом алгоритме. Аргумент на входе ФНФ называют запросом (ЗПР), а выходное значение – ответом (ОТВ) [4]. Очевидно, для некоторой интегральной схемы (либо компонента схемы) множество запросов $\{ЗПР_0, \ldots, ЗПР_{N-1}\}$ будет уникально отображено в множестве ответов $\{ОТВ_0, \ldots, ОТВ_{N-1}\}$ с помощью ФНФ.

Основная проблема безопасности использования ФНФ возникает при контрактном производстве микросхем (fabless) и заключается в потенциальной ненадежности производителя, как правило, находящейся в другой стране. В частности, использование ФНФ для защиты от контрафакта не защищает от незаконного перепроизводства изделий сверх заказанного количества (так называемая Night-Shift Problem). Кроме этого, использование ФНФ в составе реализаций криптографических алгоритмов оставляет возможность чтения пар запрос-ответ производителем [5]. Наряду с этой проблемой ФНФ также не позволяют провести идентификацию, то есть установить тождественность неизвестного РЭУ известному на основании совпадения параметров.

Для решения указанных проблем в данной работе рассматривается новый вид физически неклонируемой функции – сложный сигнальный радиопрофиль, полученный при регистрации электрической составляющей собственного электромагнитного излучения радиоэлектронных узлов РЭУ. Запросом для такой ФНФ является возмущающее воздействие на радиоэлектронный узел, а ответом – уникальный СРП.

Постановка задачи и методы исследования

Целью представленного исследования является повышение защиты радиоэлектронных устройств от неправомерного копирования и размножения, посредством исследования новой ФНФ, приобретенной при технологическом разбросе параметров электронных компонентов. Данная ФНФ связана с собственными электромагнитными излучениями радиоэлектронного устройства и отражает его индивидуальные особенности. Для достижения поставленной цели необходимо решить задачи по регистрации СРП, декомпозиции и экстракции его основных параметров, а также аутентификации и идентификации сложных радиоэлектронных узлов статистическими методами.

Для проведения исследований по идентификации необходимы экспериментальные образцы (ЭО) и измерительная аппаратура. В качестве ЭО, уникальность и тождественность которых необходимо определить по их СРП, было произведено 20 радиоэлектронных узлов. Данные РЭУ состоят из параллельно соединенных ключей на биполярном (БП) и МОП – транзисторах (рис. 1).

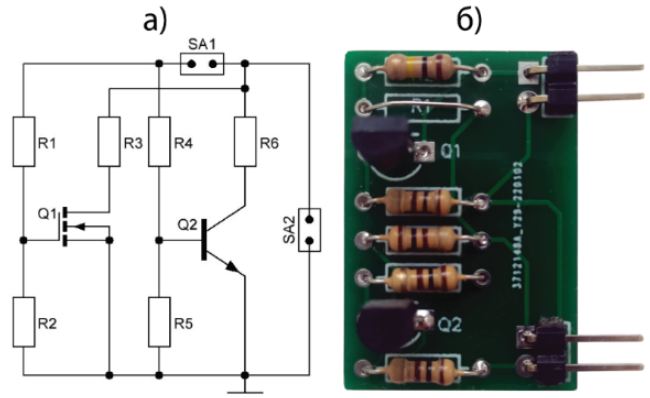


Рис. 1. Экспериментальный образец – составной радиоэлектронный узел: а) схема электрическая принципиальная, б) общий вид

Управляющее напряжение +5 В подключено к разъему *SA2*, подается на затвор МОП-транзистора *Q1* и базу БП-транзистора *Q2* посредством замыкания контактов *SA1*. *R1* – перемычка, *R2* – подтягивающий резистор 100 кОм, *R3*, *R6* – нагрузка 100 Ом, *R4*, *R5* – делитель напряжения.

Наличие фильтрующих и паразитных емкостей в ЭО при подаче управляющего напряжения ведет к перераспределению энергии между элементами фильтрации и паразитными реактивными накопителями, которое имеет колебательный характер. Затухание колебаний здесь будет зависеть от соотношения нагрузочных параметров потребителей и накопителей, причем чем меньше нагрузка потребителя, тем медленнее затухают колебания. В представленном электронном узле имеет место возникновение колебательного перераспределения энергии между накопителями в роли которых выступают емкости подзатворных диэлектриков МОП-структуры, барьерные и диффузионные емкости p-n переходов БП-транзистора. Методом решения дифференциальных уравнений в работе [6] определен вид возникающих затухающих синусоидальных колебаний:

$$U_{CB}(t) = U_0 e^{-\delta t} \sin(\omega t + \varphi),$$

где U_0 – начальная амплитуда колебаний (постоянная интегрирования, зависящая от значений параметров накопителей), δ – коэффициент затухания, ω – угловая частота колебаний, φ – начальная фаза колебаний.

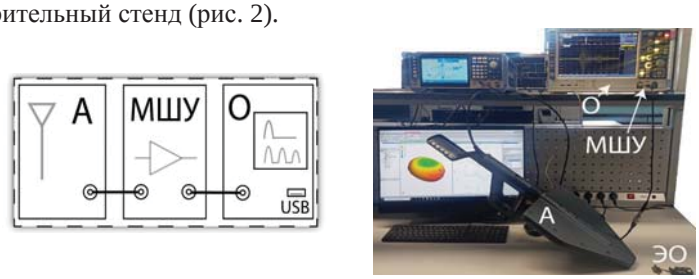
Поскольку обычно электронный узел состоит из группы компонентов, итоговый СРП узла – суперпозиция СРП входных и выходных цепей его составляющих, излучающих свободные затухающие колебания в моменты времени, соответствующие приходу управляющего импульса [7]:

$$U(t) = \sum_{i=1}^{N} U_{CBi}(t) = \sum_{i=1}^{N} U_{0i} e^{-\delta_i (t - t_{0i})} \sin[\omega_i (t - t_{0i})],$$

где t – текущий момент времени, t_0 – момент времени начала излучения i-го колебания.

Выражение (2) является основным уравнением для СРП, излучаемого электронным узлом устройства и справедливо при выполнении условия $t - t_{0i} \geq 0$, а при $t - t_{0i} < 0$: $U_{CBi} = 0$. Также в выражении (2) отсутствует начальная фаза излучения, поскольку этот параметр косвенно входит в t_0.

Излучение СРП происходит при передаче мощности от источника питания на излучающие элементы. На практике наиболее часто встречается непосредственное излучение источника, например, подводящих линий или отдельного компонента. Также встречаются излучения через подключенные кабели питания, шины данных или сигнальные линии. Для регистрации излученного СРП был построен измерительный стенд (рис. 2).



а) б)

Рис. 2. Измерительный стенд: а) блок-схема, б) фото

СРП, излученный *ЭО*, принимается широкополосной антенной *А* и усиливается *МШУ* – малошумящим сверхширокополосным усилителем. Усиленный СРП обнаруживается и регистрируется сверхбыстродействующим осциллографом реального времени *О*. Полученные в результате измерения данные передаются в персональный компьютер для дальнейшей обработки. От ширины полосы пропускания измерительной системы, разрядности и частоты дискретизации осциллографа зависит детализация исследования СРП. Для регистрации СРП длительностью более 5 нс, возможен частотный диапазон 0,1 – 3 ГГц, дискретизация 20 Гвыб/с.

Изучение СРП предполагается провести методом корреляционного анализа, полученного от исследуемого объекта СРП, отражающего его радиотехническую уникальность, с СРП аналогичного РЭУ (репером), путем построения корреляционной функции $r(h)$ [8]:

$$r(h) = \frac{\sum_{i=h}^{M+h} \left(Y_{1,i} - \bar{Y}_1\right) \cdot \left(Y_{2,i} - \bar{Y}_2\right)^{(1)}}{\sqrt{\sum_{i=h}^{M+h} \left(Y_{1,i} - \bar{Y}_1\right)^2 \cdot \sum_{i=h}^{M+h} \left(Y_{2,i} - \bar{Y}_2\right)^2}},$$

где M – число выборок («окно» преобразования), h – номер отсчета положения «окна» ($0 < h < K - M$), K – общее число отсчетов СРП, $Y_1 = \frac{U}{U_M}$ – выборки значений СРП *а*, $Y_2 = \frac{U_B}{U_{MB}}$ – выборки значений СРП *б*, $\bar{Y}_1 = \frac{1}{M} \sum_{i=h}^{M+h} Y_{1,i}$, $\bar{Y}_2 = \frac{1}{M} \sum_{i=h}^{M+h} Y_{2,i}$ – средние значения выборок, U – значение СРП *а* в точке выборки, U_M – максимальное значение СРП *а*, U_B – значение СРП *б* в точке выборки, U_{MB} – максимальное значение СРП *б*.

Анализ по определению идентичности СРП предполагается провести методом декомпозиции, представленным в работе [9], с экстракцией параметров посредством частотно-временного преобразования:

$$X(f, h) = \sum_{h=0}^{K-O} \left[\sum_{c=h}^{O-1+h} U(O) \exp\left(- j \frac{2\pi f c}{O} \right) \right],$$

где $X(f, h)$ – дискретный частотно-временной спектр сигнала, $U(O)$ – сигнал, дискретизированный во времени, c – номер отсчета, f – частота, O – число точек, образующих «окно» преобразования.

Полученные результаты

В результате проведенных испытаний было получено 20 СРП, от каждого экспериментального образца по одному. За репер принят СРП ЭО № 1. Вид репера и его корреляционный анализ с СРП случайным образом выбранного ЭО № 12, представлен на рисунке 3.

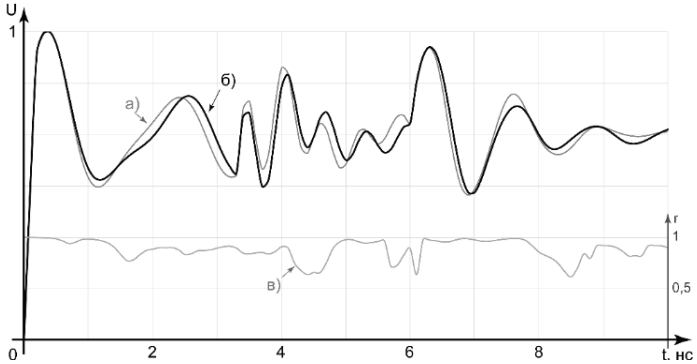


Рис. 3. СРП: а) репер, б) образец № 12, в) корреляционная функция

Как видно из данного рисунка корреляционная функция на временной оси опускается ниже 0,9, достигая 0,6, что по шкале Чеддока [10] означает заметную корреляционную связь (кривые похожи). Таким образом, прослеживается некая тождественность между СРП.

Аналогично был проведен корреляционный анализ СРП для каждого из представленных образцов. Для детального исследования тождественности СРП (то есть идентификации) была проведена декомпозиция СРП и по частотно-временному спектру (рис. 4) получены основные параметры СРП.

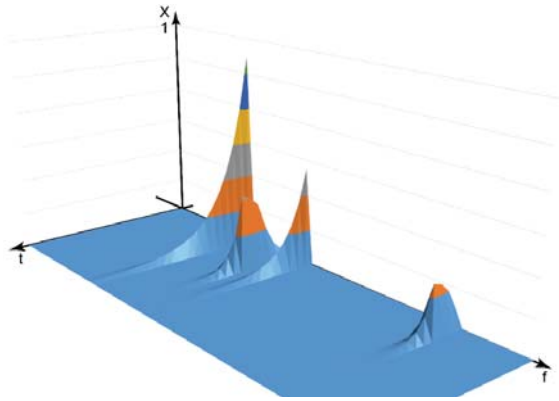


Рис. 4. Частотно-временной спектр СРП

Как видно из рисунка 4, СРП состоит из четырех излучателей (N = 4). После операции декомпозиции (в работе [9] подробно описана операция декомпозиции и экстракции) возможно получить таблицу параметров данных излучателей.

Таблица 1

Параметры излучателей репера

Излучатели	f, ГГц	δ, нс$^{-1}$	t_0, нс	U_0
i=1	0,68	-0,31	0	0,84
i=2	0,98	-0,43	0	0,4
i=3	0,86	-0,75	5,3	0,96
i=4	1,8	-0,85	3,1	0,73

Экстракция параметров, представленных в выражении (2), при декомпозиции позволяет найти число элементарных излучателей N, участвующих в создании СРП. В случае, если N полученного СРП меньше, чем число излучателей репера N_P, то следует делать вывод о выходе из строя некоторых компонентов интересующего узла, либо о некорректном производстве измерения. Принять решение в данной ситуации поможет совокупность параметров СРП. В случае равенства – все элементы узла участвуют в излучении. При превышении числа излучателей в тестовом СРП по сравнению с репером, можно говорить о неверном вычислении данного параметра, либо некорректном производстве измерения. Только в случае равенства числа излучателей репера и исследуемого СРП можно говорить о дальнейшем проведении идентификации.

При принятии решения по идентификации возможно воспользоваться критерием согласия Пирсона, применяемом для проверки гипотезы о соответствии эмпирического распределения предполагаемому теоретическому распределению [11]:

$$\chi^2 = \sum_{j=1}^{k} \frac{(u_j - e_j)^2}{e_j},$$

где u_j – наблюдаемая частота признака в j-й группе, e_j – теоретическая частота признака в j-й группе.

Данный критерий может быть использован для любых видов функций, даже при неизвестных значениях их параметров, что обычно имеет место при анализе результатов испытаний. Для применения критерия согласия Пирсона необходимо построить таблицу соответствия параметров (табл. 2), полученных в результате декомпозиции СРП.

Таблица 2

Таблица соответствия параметров

Излучатели / Параметры	*i=1*	*i=2*	*i=3*	*i=4*	u_j	e_j
f	1	1	1	1	4	4
δ	1	0	1	1	3	4
t_0	1	1	1	1	4	4
U_0	1	1	0	1	3	4

В таблице 2 показано четыре излучателя i (N = 4), и результат попадания параметров данных излучателей в доверительный интервал (*1* – параметр попал в доверительный интервал, *0* – параметр не попал в доверительный интервал). Сам доверительный интервал был получен в результате проведения многочисленных натурных испытаний и представляет собой не что иное, как технологический разброс параметров. Доверительный интервал также может быть определен по результатам моделирования, либо в результате расчетов по известным справочным данным. Значение u_j – сумма реальных попаданий параметров излучателя в доверительный интервал, e_j – сумма ожидаемых попаданий параметров излучателя в доверительный интервал (для N = 4, e_j = 4).

Используя выражение (4) совместно с таблицей 2 рассчитывается коэффициент χ^2. Для случая, представленного на рисунке 3, $\chi^2 \approx 0{,}97$. Результаты эмпирических исследований показывают, что χ^2 есть вероятность тождественности исследуемого СРП и репера. Таким образом, СРП, представленные на рисунке 3 тождественны с вероятностью 97% (РЭУ принадлежат одной группе с данной вероятностью). Анализ показал, что все исследуемые образцы идентифицированы и тождественны реперу с вероятностью не менее 95% ($\chi^2 \geq 0{,}95$).

Следует заметить, что при проведении эксперимента для анализа также был снят СРП образца № 1 (рис. 5).

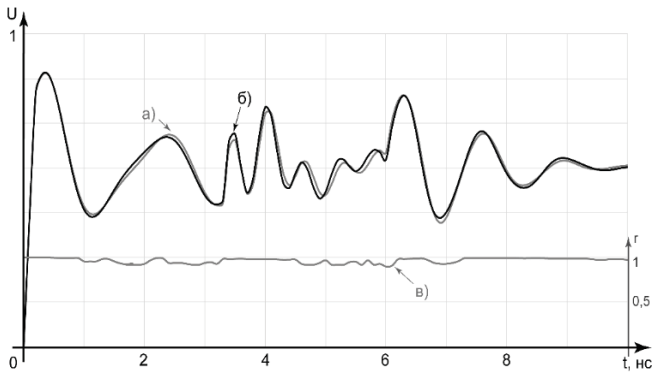


Рис 5. СРП: а) репер, б) образец № 1, в) корреляционная функция

Как видно из данного рисунка корреляционная функция не опускается ниже 0,9, что по шкале Чеддока означает весьма высокую корреляционную связь (кривые идентичны).

Таким образом, можно говорить об аутентификации исследуемого образца, то есть исследуемый образец и есть репер.

Методика проведения идентификации

Полученные при проведении эксперимента данные имеют сходство с данными, полученными в результате моделирования [12], что говорит о высокой воспроизводимости метода радиосенсорной идентификации. Корреляционный анализ при исследовании СРП позволяет провести аутентификацию РЭУ, то есть определить его подлинность. В данном случае СРП – уникальная ФНФ радиоэлектронного устройства. Аутентификация невозможна, если корреляционная функция на временной оси СРП опускается ниже 0,9. При построении таблицы соответствия параметров и использовании коэффициента согласия Пирсона можно провести идентификацию РЭУ с интересующей исследователя вероятностью. Однако критически обсуждая полученные результаты, автор не рекомендует идентифицировать устройство при $\chi^2 < 0{,}95$, но выбор всегда остается за исследователем.

По результатам исследований можно привести методику проведения идентификации РЭУ радиосенсорным методом (рис. 6).

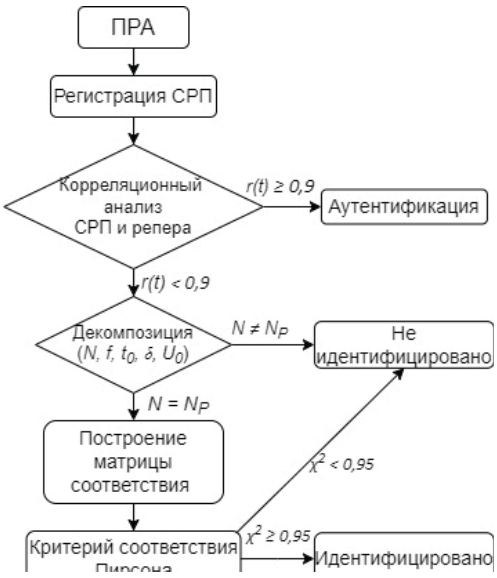


Рис. 6. Методика проведения идентификации РЭУ радиосенсорным методом

Как видно из представленного рисунка идентификация и аутентификация возможны только при равенстве числа излучателей исследуемого устройства и репера. В противном случае границы применимости метода заканчиваются, поскольку исходные данные ошибочны, либо исследуемое устройство находится не в функциональном состоянии.

Заключение

В работе представлена физически неклонируемая функция, основанная на сигнальном радиопрофиле, полученном при регистрации электрической составляющей ближнего поля электромагнитного излучения РЭУ. Данная ФНФ приобретена изделием в процессе производства, вследствие технологических допусков на параметры комплектующих компонентов. Восстановление и анализ таких СРП по взаимной корреляции с репером, в сочетании критерием согласия Пирсона при декомпозиции и экстракции параметров, позволяет проводить не только аутентификацию, но и идентификацию РЭУ, что не может на сегодняшний день ни одна из известных ФНФ. Практическая применимость данного метода заключается в возможности отличать оригинальное радиоэлектронное изделие от контрафакта дистанционно, не вмешиваясь в функционирование прибора. Сама технология радиосенсорной идентификации позволяет использовать для анализа программно-конфигурируемые радиосистемы, что должно значительно ускорить процесс распознания, открывая дальнейшие перспективы в области развития направления ФНФ, защиты, аутентификации и идентификации радиоэлектронных устройств в целом.

Литература

1. *Федорец В.Н., Белов Е.Н., Балыбин С.В.* Технологии защиты микросхем от обратного проектирования в контексте информационной безопасности. М.: Рекламно-издательский центр «Техносфера», 2019. 216 с.

2. *Herder C., Yu M., Koushanfar F., Devadas S.* Physical Unclonable Functions and Applications // A Tutorial in Proceedings of the IEEE, 2014. P. 1126-1141. https://doi.org/10.1109/JPROC.2014.2320516

3. *Su Y., Holleman J., Otis B.* A 1.6pJ/bit 96% Stable Chip-ID Generating Circuit using Process Variations // IEEE International Solid-State Circuits Conference. Digest of Technical Papers, 2007. P. 406-611. https://doi.org/10.1109/ISSCC.2007.373466.

4. *Kim J., Patel M., Hassan H., Mutlu O.* The DRAM Latency PUF: Quickly Evaluating Physical Unclonable Functions by Exploiting the Latency-Reliability Tradeoff in Modern Commodity DRAM Devices // IEEE International Symposium on High Performance Computer Architecture (HPCA), 2018. P. 194-207, https://doi.org/10.1109/HPCA.2018.00026.

5. *Семенов А.В., Костюк А.В.* Защита ключей микросхем на физически неклонируемых функциях в условиях недоверия к кремниевой фабрике // Вопросы защиты информации, 2015. № 2(109). С. 63-68.

6. *Бойков К.А.* Моделирование и анализ колебательного перераспределения энергии при собственных электромагнитных излучениях в ключевых радиоэлектронных схемах на МОП-транзисторах // Журнал радиоэлектроники [электронный журнал], 2021. №6. https://doi.org/10.30898/1684-1719.2021.6.14.

7. *Бойков К.А.* Определение параметров электронных устройств методом пассивной радиосенсорной технической диагностики // Известия высших учебных заведений России. Радиоэлектроника, 2021. Т. 24. №6. С. 63-70. https://doi.org/10.32603/1993-8985-2021-24-6-63-70.

8. *Huang R., Cui H.* Consistency of chi-squared test with varying number of classes // Journal of Systems Science and Complexity, 2015. № 28(2). – P. 439-450. https://doi.org/10.1007/s11424-015-3051-2

9. *Бойков К.А.* Декомпозиция сигнального радиопрофиля в пассивной радиосенсорной технической диагностике и аутентификации электронных устройств // Вестник Воронежского государственного технического университета, 2022 Т. 18. № 1. С. 129-134.

10. *Шкодун П.К.* Разработка комплекса диагностических параметров оценки технического состояния тяговых электродвигателей подвижного состава // Известия Транссиба, 2020. № 4(44). С. 56-65.

11. *Thanh T.K., Vinh T.T.* The application of correlation function in forecasting stochastic processes // Herald of Advanced Information Technology, 2019. № 2(4). P. 268-277. https://doi.org/10.15276/hait04.2019.3

12. *Бойков К.А.* Схемотехническое и электродинамическое моделирование колебательного процесса перераспределения энергии в биполярном транзисторе // Известия ЮФУ. Технические науки, 2021. № 7. С. 19-31.

RADIOSENSOR IDENTIFICATION AND AUTHENTICATION OF RADIO-ELECTRONIC DEVICES

Konstantin A. Boikov, *MIREA – Russian Technological University, Moscow, Russia,* ***nauchnyi@yandex.ru***

Abstract

The presented work is devoted to the study of a new physically unclonable function (PUF) associated with the intrinsic electromagnetic radiation of a radio electronic device. This PUF arises as a result of the technological spread of the parameters of electronic components. The relevance of this study is explained by the fact that modern methods of protecting radio-electronic products from illegal cloning have a number of serious drawbacks associated with increased power consumption, the use of processor time, and the need for galvanic access to the object of study. Partially, these problems are eliminated by PUF, which allow authentication of a radio-electronic device. However, this kind of protection also has serious vulnerabilities in the case of illegal overproduction of products in excess of the ordered quantity. In addition, the PUF does not allow for the identification of radio-electronic products. The purpose of this work is to increase the protection of radio electronic devices from illegal cloning, by studying a new PUF. The work uses experimental research methods to record the electrical component of the electromagnetic field emitted by the product - the signal radio profile (SRP). Correlation analysis methods for product authentication, Pearson's statistical agreement method for identification. SRPs registered from specially designed experimental samples are presented, a correlation analysis of SRP data is carried out. To decompose and extract the parameters of the SRP, its time-frequency spectrum was constructed. A correspondence table was compiled and an analysis of Pearson's agreement was carried out. The results obtained showed the possibility of using the SRP as a new physically unclonable function that allows the identification of radio electronic devices with a probability specified by the researcher, which determines the novelty of the work. It has been established that with Pearson's coefficient of agreement between the parameters of the studied SRP and the benchmark of more than 0.95, a radio-electronic device can be reliably identified. The practical significance of the work lies in the possibility of using the SRP to identify a group of devices and radio-technical protection of a radio-electronic product from fakes and illegal copies.

Keywords: *signal radioprofile, Pearson criterion, frequency-time transformation, radiosensor identification, correlation analysis, decomposition.*

References

1. V. N. Fedorets, E. N. Belov, S. V. Balybin (2019). Technologies for protecting microcircuits from reverse engineering in the context of information security. Moskow: Reklamno-izdatel'skiy tsentr "Tekhnosfera". 216 p. (In Russian)

2. C. Herder, M. Yu, F. Koushanfar, S. Devadas (2014). Physical Unclonable Functions and Applications. *A Tutorial in Proceedings of the IEEE*, 2014, pp. 1126-1141. https://doi.org/10.1109/JPROC.2014.2320516

3. Y. Su, J. Holleman, B.A. Otis (2007). 1.6pJ/bit 96% Stable Chip-ID Generating Circuit using Process Variations. *IEEE International Solid-State Circuits Conference. Digest of Technical Papers,* pp. 406-611. https://doi.org/10.1109/ISSCC.2007.373466.

4. J. Kim, M. Patel, H. Hassan, O. Mutlu (2018). The DRAM Latency PUF: Quickly Evaluating Physical Unclonable Functions by Exploiting the Latency-Reliability Tradeoff in Modern Commodity DRAM Devices. *IEEE International Symposium on High Performance Computer Architecture (HPCA)*, 2018, pp. 194-207, https://doi.org/10.1109/HPCA.2018.00026.

5. A.V. Semenov, A.V. Kostyuk (2015). Protecting the keys of microcircuits on physically non-clonable functions in conditions of distrust of the silicon factory. *Voprosy zashchity informatsii.* No. 2(109), pp. 63-68. (In Russian)

6. K.A. Boikov (2021. Modeling and analysis of oscillatory redistribution of energy at own electromagnetic radiations in key radio-electronic circuits on MOSFETs. *Zhurnal radioelektroniki*. No. 6. https://doi.org/10.30898/1684-1719.2021.6.14. (In Russian)

7. K.A. Boikov (2021). Determination of the parameters of electronic devices by the method of passive radio-sensor technical diagnostics. *Izvestiya vysshikh uchebnykh zavedeniy Rossii. Radioelektronika*. Vol. 24. No. 6, pp. 63-70. https://doi.org/10.32603/1993-8985-2021-24-6-63-70. (In Russian)

8. R. Huang, H. Cui (2015). Consistency of chi-squared test with varying number of classes. *Journal of Systems Science and Complexity*. No. 28(2), pp. 439-450. https://doi.org/10.1007/s11424-015-3051-2.

9. K.A. Boikov (2022). Decomposition of the signal radio profile in passive radio sensor technical diagnostics and authentication of electronic devices // Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. Vol. 18. No. 1, pp. 129-134. (In Russian)

10. P.K. Shkodun (2020). Development of a set of diagnostic parameters for assessing the technical condition of traction electric motors of rolling stock. *Izvestiya Transsiba*. No. 4 (44), pp. 56-65. (In Russian)

11. T.K. Thanh, T.T. Vinh (2019). The application of correlation function in forecasting stochastic processes. *Herald of Advanced Information Technology*. No. 2(4), pp. 268-277. https://doi.org/10.15276/hait04.2019.3. (In Russian)

12. K.A. Boikov (2021). Circuitry and electrodynamic modeling of the oscillatory process of energy redistribution in a bipolar transistor // Izvestiya YUFU. Tekhnicheskiye nauki. No. 7, pp. 19-31. (In Russian)

Information about author:

Konstantin A. Boikov, *Candidate of Technical Sciences, Associate Professor of the Department of Radio Wave Processes and Technologies of the Institute of Radioelectronics and Informatics of the Federal State Budgetary Educational Institution of Higher Education "MIREA – Russian Technological University", Moscow, Russia*