УДК 621.3.082.74 DOI: 10.31114/2078-7707-2020-4-225-230

Модель выявления контрафактных восстановленных микросхем СОЗУ с помощью ускоренного старения

В.Н. Старцев, А.В. Семенов

ФГУП «18 ЦНИИ» МО РФ, г.Москва, memory.test@ya.ru

***Аннотация* — В статье предложена модель, позволяющая выявить микросхемы СОЗУ, бывшие в употреблении, на основе динамики увеличения количества нестабильных ячеек памяти в результате воздействия ускоренного старения процесса деградации полупроводников NBTI.**

***Ключевые слова* — контрафакт, ускоренные испытания на безотказность, NBTI, статическое ОЗУ.**

I. Введение

Существует много видов контрафактных микросхем: микросхемы, не отвечающие заявленным техническим характеристикам, дефектные микросхемы, перемаркированные микросхемы и оригинальные микросхемы, бывшие в употреблении, восстановленные и проданные как новые. Категория восстановленных микросхем составляет около 80% от всей контрафактной продукции микроэлектроники [1]. Этот класс контрафакта приводит к преждевременному выходу из строя создаваемых на их основе изделий, т.е. фактический жизненный цикл микросхемы заканчивается раньше, чем декларируемый. Это наносит урон надежности и безопасности функционирования аппаратуры [2]. При этом именно такие микросхемы сложно выявлять, так как они, зачастую успешно проходят функциональный контроль.

Кроме этого, продолжительность жизненного цикла некоторых радиоэлектронных систем превышает жизненный цикл микросхем, которыми они комплектуются. В этом случае вероятность комплектования аппаратуры контрафактными микросхемами растет. С учетом неопределенности источников и цепочек поставок и несовершенства методов выявления контрафактных микросхем угроза их попадания в оборудование критически важных технических систем – это реальная проблема надежности, качества и безопасности продукции.

Существующие меры, направленные на борьбу с контрафактными изделиями микроэлектроники: обязательная маркировка с серийным номером изделия, электронный идентификатор микросхемы (Electronic Chip ID) [3, 4], использование уникальных особенностей изделий микроэлектроники, например физически неклонируемые функции («отпечатки пальцев» в области техники) [5-7], и др. позволяют определить только подлинность изделия за счет сравнения считанной идентификационной информации с априорной из информационных источников производителя или испытательной лаборатории.

Подавляющее число методов решает задачу подтверждения подлинности микросхемы, но не позволяет выявить подлинные микросхемы, бывшие в употреблении.

Параметрический контроль для поиска контрафактных микросхем мог бы быть более эффективным при наличии эталона (достоверно новой, неиспользованной оригинальной микросхемы), однако отсутствие такового делает методы, основанные на сравнении с эталоном, не достоверными для выявления восстановленных изделий [8].

Полноценные испытания на безотказность являются продолжительными и дорогостоящими, поэтому несмотря на высокую достоверность не могут рассматриваться, как удовлетворительное решение задачи [9].

В этой связи разработка моделей и методов поиска контрафактных восстановленных микросхем, не требующих эталонов, является актуальной.

II. Известные результаты

Известны технические решения, которые позволяют определить микросхемы, бывшие в употреблении, на основе внедрения (на этапе проектирования) в кристаллы микросхем сенсоров (аппаратных одометров) [10-11], реагирующих на процессы старения полупроводников. Такие одометры состоят из двух одинаковых электрических цепей на кристалле, одна из которых обособлена (опорная), а вторая испытывает нагрузку во время работы микросхемы (деградирующая). Сравнительный анализ аналоговых характеристик цепей дает возможность установить факт и примерное время использования микросхем. В различных исполнениях данные электрические цепи состоят из генераторов колебаний [10], инверторов [11], внутренних проводников микросхемы [12] и др. Данные решения, помимо издержек в виде дополнительного места на кристалле, часто требуют привлечения точных измерительных схем (реализованных на кристалле или вне его). Кроме того, микросхемы с такими сенсорами на практике редко встречаются.

Другая группа решений основана на записи данных счетчика (или сенсора старения) микросхемы в ее нестираемую память (ПЗУ) [13-15]. Например [14], предлагается записывать в нестираемую память

микросхемы информацию о времени ее эксплуатации, а также время и место ее производства, дополнительную информацию, считанную из различных сенсоров, обеспечивающих данными о состоянии надежности и функциональности микросхемы. Данный подход представлен в виде цифрового решения и не требует привлечения аналогового измерительного оборудования, однако по-прежнему остаются издержки проектирования и выделения дополнительного места на кристалле для реализации такого подхода.

Многие микросхемы, использующиеся для вычислений, имеют в своем составе оперативные запоминающие устройства (ОЗУ). Существуют физически неклонируемые функции микросхем на базе статического ОЗУ, чувствительные к процессам деградации [16]. При этом потребителю необходимо считать данные из микросхемы, сопоставить полученный результат с информацией, предоставляемой производителем – сравнительный анализ позволяет сделать вывод, была микросхема в употреблении или нет.

Преимущество подхода в том, что он не требует реализации дополнительных механизмов на кристалле, однако необходимо иметь априорную информацию от производителя.

Старение полупроводниковых структур проявляется в виде сдвига физических параметров, таких как активная проводимость, подвижность носителей заряда, периодичность тока и др. Сдвиги этих физических параметров транзистора с высокой точностью моделируются одним параметром, а именно, сдвигом минимального уровня напряжения, которое нужно приложить к базе транзистора, чтобы открыть полупроводниковый канал для прохождения электрического тока от истока к стоку. Речь идет о пороговом напряжении «threshold voltage» (V_{th}). Причем, запас для сдвига V_{th} до критического значения, при котором транзистор уже не может менять свое состояние, составляет жизненный ресурс транзистора и, соответственно, микросхемы как ее базового элемента.

На устранение требования к наличию априорной информации, без необходимости внедрения датчика старения, без эталона, с учетом снижения трудоемкости испытаний, направлена предлагаемая модель.

Гипотеза исследования заключается в том, что методы ускоренного старения для цифровых схем статического ОЗУ [17] имеют устойчивое влияние на скорость изменения параметров статистических распределений, определяющих «новые» микросхемы (не подвергшиеся значительной деградации) и микросхемы, бывшие в употреблении (исчерпавших значительное количество ресурса).

III. Модель выявления микросхем, бывших в употреблении

Открыто и исследовано множество деградационных процессов полупроводниковых транзисторов, одним из самых значимых среди них в современной научной литературе признают негативное смещение температурной неустойчивости (в английской аббревиатуре «NBTI»).

Влияние NBTI эффекта на работоспособность транзистора моделируется через его электрические и геометрические параметры следующим выражением:

$$\Delta V_{th} = A \cdot \exp\left(\frac{E_a}{k_B \cdot T}\right) V_{gs}^{b} \cdot t_{stress}^{n} \cdot \frac{1+C}{W}, \qquad (1)$$

где ΔV_{th} – смещение порогового напряжения включения транзистора,

V_{gs} – напряжение на затворе транзистора,

W – ширина транзистора,

T – среднестатистическая температура в период эксплуатации,

A, E_a, k_B, b, n, C – константы из реакционно-диффузионной модели описания NBTI эффекта,

t_{stress} – время воздействия NBTI процесса на транзистор, меньше либо равно периоду эксплуатации.

Уравнение (1) на практике имеет много неизвестных величин, что не позволяет решить его относительно времени стресса, ассоциируемого с периодом эксплуатации. К примеру, невозможно измерить и установить абсолютное значение ΔV_{th} транзисторов готовой микросхемы.

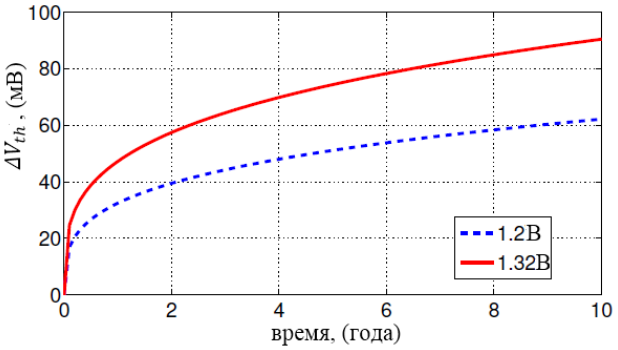

Рис. 1. Деградационные кривые смещения порогового напряжения включения транзисторов под воздействием NBTI процесса в течении жизненного цикла микросхем с напряжением питания 1,2 В и 1,32 В

Рассмотрим производную, заметим, что правая часть выражения (1) – степенная функция от времени: $K \cdot t_{stress}^{n}$, где K – постоянный коэффициент, $K = A \cdot \exp\left(\frac{E_a}{k_B \cdot T}\right) V_{gs}^{b} \cdot \frac{1+C}{W}$, значение степени которой не равно единице (рис. 1); в различных источниках [18] оно варьируется между 0,11 и 0,3. Поэтому зависимость от времени стресса и нелинейность функции дают принципиальную возможность выразить время, ассоциируемое с периодом эксплуатации через производную:

$$t_{stress} = \sqrt[n-1]{\frac{(\Delta V_{th})'}{K \cdot n}} \quad . \qquad (2)$$

Однако уравнение (2) на практике также неразрешимо. Для того чтобы фиксировать скорость смещения порогового напряжения $(\Delta V_{th})'$ конкретного транзистора микросхемы необходимо локально воздействовать на него стрессом и напрямую измерять его аналоговые электрические характеристики. При этом транзисторы в микросхемах находятся в составе целых завершенных электрических цепей, которые в большинстве своем обособлены от внешних контактов дешифраторами, компараторами и другими интерфейсными, терминальными электрическими схемами. Таким образом, невозможно воздействовать локально стрессом на конкретный транзистор, чтобы не изменить электрические параметры всей цепи и невозможно напрямую измерить его аналоговые электрические характеристики без дополнительных заранее спроектированных электрических цепей на кристалле, адаптированных для этих нужд. Соответственно, дополнительные электрические цепи - не выход для решения поставленной задачи, так как в таком случае целесообразней и эффективней будет реализовать аппаратный одометр, описанный выше. В свою очередь, коэффициент K складывается из данных о электрических и геометрических параметрах транзистора и констант из реакционно диффузионной модели описания NBTI эффекта, причем некоторые из этих констант возможно настроить только посредством эксперимента с учетом того, что известно смещение ΔV_{th} и время стресса, что создает замкнутый круг проблем. Таким образом, установить закон деградации готовой микросхемы без дополнительных, предназначенных для этой цели электрических цепей на практике представляется невыполнимой задачей.

Автором Dapartz предложен подход [19], позволяющий оценить среднее смещение ΔV_{th} в готовой микросхеме статического ОЗУ через увеличение количества нестабильных ячеек ее массива памяти под воздействием деградационного процесса NBTI. Физически подход основан на нестабильности ячейки статического ОЗУ, выражаемой в самопроизвольном переключении ее логического состояния в режиме считывания или хранения при редуцировании напряжения питания, связанной с разницей уровней пороговых напряжений включений транзисторов (V_{th}) инверторов ядра ячейки статического ОЗУ, отвечающих за удержание логических состояний. Данная разница уровней пороговых напряжений открытия транзисторов инверторов предопределяет включение определенного логического состояния ячейки статического ОЗУ, к которому она стремится при понижении напряжения питания ядра ячейки в режиме чтения или хранения. Причем, чем больше разница напряжений, тем сильней ячейка статического ОЗУ стремится к своему предпочтительному логическому состоянию, соответственно, выше ее нестабильность. В конечном итоге это приводит к самопроизвольному переключению логического состояния даже при небольшом понижении напряжения питания, тогда как ячейки с меньшей разницей уровней напряжения включения транзисторов (и, соответственно, инверторов) самопроизвольно переключаются при большем падении напряжения питания.

Упомянутая разница уровней напряжения открытия транзисторов (включения инверторов) обусловлена вариативностью (разбросом) технологического процесса изготовления и старением транзисторов инверторов ячейки статического ОЗУ.

Для микросхем статического ОЗУ от 65 нм и больше установлена линейная зависимость сдвига порогового напряжения открытия транзисторов и увеличения числа нестабильных бит [20]. Таким образом, после стресса:

$$\Delta V_{th} \approx c \cdot N_{bit}\,, \qquad (3)$$

где c – установленный коэффициент пропорциональности, в работе [21] имеет приближенное значение около 3, N_{bit} – число увеличившихся после NBTI стресса нестабильных бит памяти.

Выражение (1) можно записать в виде:

$$K \cdot t_{stress}^{n} \approx c \cdot N_{bit}\,. \qquad (4)$$

Таким образом, неизвестное неизмеримое в готовой микросхеме среднее смещение пороговых напряжений включения транзисторов тождественно заменено на легко измеряемое цифровым способом количество увеличившихся нестабильных бит СОЗУ после стресса продолжительностью t_{stress} .

При этом по-прежнему неизвестны коэффициенты K и n, что не позволяет вычислить искомое время стресса, поэтому целесообразно рассмотреть следующее выражение:

$$\frac{\Delta V_{th_k}}{\Delta V_{th_k+1}} = \frac{t_{stress_k}^{n} - t_{stress_{k-1}}^{n}}{t_{stress_{k+1}}^{n} - t_{stress_k}^{n}} \approx \frac{N_{bit_k}}{N_{bit_{k+1}}}\,, \qquad (5)$$

где ΔV_{th_k} – среднее смещение пороговых напряжений открытия транзисторов микросхемы СОЗУ после k-го испытания стрессом;

$t_{stress_k}^{n}$ – общее время стресса после k-го испытания;

N_{bit_k} – число увеличившихся нестабильных бит после k-го испытания.

В выражении (5) получена связь времени стресса и динамики увеличения числа нестабильных бит статического ОЗУ после него без уточнения коэффициента K.

Отметим, что дробь $\frac{t^n_{stress_k} - t^n_{stress_{k-1}}}{t^n_{stress_{k+1}} - t^n_{stress_k}}$ – монотонно убывающая функция с асимптотой, равной 1, для всех возможных n из источников описания NBTI модели, при этом значения $1+\varepsilon$, где $0<\varepsilon \ll 1$, функция достигает на начальном отрезке, на этапе насыщения процесса NBTI, так что интеграл от определенного периода начального отрезка функции (от $t_0=0$) для всех n реакционно-диффузионной модели значительно больше интегралов такого же периода последующих отрезков (рис. 2), что удобно использовать в качестве решающего правила для идентификации начального/не начального отрезка деградационной кривой, на котором находится статическое ОЗУ, что позволяет построить решающее правило.

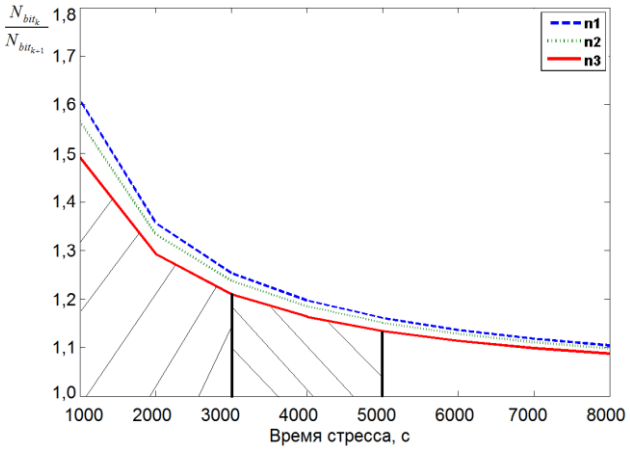

Рис. 2. Изменение отношения количеств увеличившихся нестабильных бит СОЗУ смежных периодов стресса от общего времени деградации микросхемы с различными степенями реакционно- диффузионной модели NBTI (n_1=0.25, n_2=0.16, n_3=0.11)

В связи с дискретной природой измеряемых для расчета данных (числа увеличившихся после стресса нестабильных бит) имеет смысл использовать сумму вместо интеграла: $\sum_{k=2}^{\lim} \frac{(k\cdot\tau)^n - ((k-1)\cdot\tau)^n}{((k+1))^n - (k\cdot\tau)^n}$, где τ – период ускоренного старения микросхемы, $\tau = t^n_{stress_k} - t^n_{stress_{k-1}}$, k – итерация цикла «ускоренное старение – считывание», $k\geq 2$. Рассмотрим следующие значения степени n реакционно-диффузионной модели NBTI: n_1=0.25 , n_2=0.16, n_3=0.11 из источников [18-20]:

$$\sum_{k=1}^{5} \frac{k^{n_1} - (k-1)^{n_1}}{(k+1)^{n_1} - k^{n_1}} = 5{,}1517 < \sum_{k=1}^{5} \frac{k^{n_2} - (k-1)^{n_2}}{(k+1)^{n_2} - k^{n_2}} < \sum_{k=1}^{5} \frac{k^{n_3} - (k-1)^{n_3}}{(k+1)^{n_3} - k^{n_3}}$$

На рис. 2 заштрихованы две соседних области стресса.

Таким образом, функция с большим значением n принимает меньшее значение, поэтому решающим правилом может стать выражение $\sum_{k=1}^{5} \frac{N_{bit_k}}{N_{bit_{k+1}}} \geq 5{,}1517$, истинность которого может говорить о том, что микросхема «новая», а значение «ложно» – о том, что микросхема «восстановленная».

Для практической реализации модели необходимо в определенном логическом положении ячеек статического ОЗУ подвергнуть микросхему NBTI стрессу в течении фиксированного периода времени τ, после чего редуцировать шагами напряжение питания микросхемы до нулевого уровня, причем после каждого шага подсчитывать количество нестабильных ячеек (количество бит, изменивших свое логическое состояние в режиме чтения N_{bit}), при этом цикл «стресс-подсчет N_{bit} » проводится k раз, $k \geq 2$, после чего возможно применить описанное выше правило.

IV. Обсуждение результатов и выводы

Предлагаемая модель может работать не только в микросхемах статического ОЗУ, но и в других сложно-функциональных классах микросхем, таких как микроконтроллеры, ПЛИС и другие. При этом необходимая продолжительность стрессовых воздействий может вычисляться экспериментально для различных типов изделий.

Основным результатом использования предложенной модели является выявление восстановленных микросхем, содержащих статическое ОЗУ, простым цифровым оборудованием без применения точных аналоговых измерительных приборов, посредством штатного интерфейса микросхемы, без специальных требований к ее электрической и топологической схеме, без априорной первичной информации о ее физико-технологических свойствах.

Литература

[1] ГОСТ Р 57880-2017. Система защиты от фальсификаций и контрафакта. Изделия электронные. Предотвращение получения, методы обнаружения, сокращение рисков применения и решение по использованию фальсифицированной и контрафактной продукции [Текст]. – Введ. 31-10-2017. – Москва : Федеральное агентство по техническому регулированию и метрологии ; М. : Стандартинформ, 2017.

[2] Guin, U. et al. Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead // Journal of Electronic Testing. – February 2014.

[3] Arndt K. et al. Reliability of laser activated metal fuses in drams // Proc. of IEEE on Electronics Manufacturing Technology Symposium, 1999, pp. 389– 394.

[4] Robson N. et al. Electrically programmable fuse (efuse): From memory redundancy to autonomic chips // Proc. of IEEE on Custom Integrated Circuits Conference, 2007, pp. 799–804.

[5] Pappu, R. Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / R. Pappu // Massachusetts Institute of Technology (MIT). – Cambridge, 2001. – 154 p.

[6] Suh G., Devadas S. Physical unclonable functions for device authentication and secret key generation // Proc. of

ACM/IEEE on Design Automation Conference, June 2007, pp. 9 –14.
[7] Kursawe K. et al. Reconfigurable physical unclonable functions - enabling technology for tamper-resistant storage // Proc. of IEEE International Workshop on Hardware-Oriented Security and Trust, July 2009, pp. 22 –29.
[8] Семенов А. В., Старцев В. Н., Степанов Е.Н. Технометрическая идентификация микросхем для контроля жизненного цикла и поиска контрафакта // Проблемы разработки перспективных микро-и наноэлектронных систем (МЭС). – 2018. – No. 4. – С. 143-148.
[9] Архипова И. В., Батурин А. В., Левин Р. Г., Митюшов А. И. Апробация методики оценки показателей надежности электронной компонентной базы для систем управления по результатам испытаний малых выбо -рок ПЛИС фирмы Altera // Вопросы радиоэлектроники. 2017. № 7. С. 87–92.
[10] Pat. US 7592876 B2 USA, Int. Cl. HO3K 3/03, GOIR 3L/26. Leakage oscillator based aging monitor / Paul F. Newman ; Intel Corporation, Santa Clara, CA (US). – appl. №.:11/298,018 ; filed Dec. 8, 2005; date of Patent Sep. 22, 2009.
[11] Savanur P., Tragoudas S. A Method to Determine the Static NBTI Stress Time of Embedded Component in an Integreted Circuit // VALID 20176: The Ninth International Conference on Advances in System Testing and Validation.
[12] Pat. US 2017/O126229 A1 USA, Int. Cl. HO3K 9/003, HOIL 23/525, GOIR 3L/28, GITC 17/18. On-chip aging sensor and counterfeit integrated circuit detection method / Tan S. et al. ; Riverside, CA (US). – appl. №. 15/338,170, filed Oct. 28, 2016, Pub. Date May 4, 2017.
[13] Bhuvaneswari M. et al. Recycled IC Detection Based on AF and RO Sensors for Security and Reliability // International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Special Issue 6, May 2015 pp. 500-506.
[14] Pat. EP0623900A1, Int. Cl. G07C3/00. Recycable component with data storage for storing information for examining the component and product including such a component / Scheidt L. et al.; Sony International (Europe). – appl. №. EP0623900A1, filed 1994-11-09, Pub. Date 2004-03-10.
[15] Zhang X., Tehranipoor M. Design of On-chip Light-weight Sensors for Effective Detection of Recycled ICs // IEEE Transactions on VLSI (TVLSI), 2013.
[16] Gao Y., et al. Detecting Recycled Commodity SoCs: Exploiting Aging-Induced SRAM PUF Unreliability // Preprint submitted to Integration, The VLSI Journal. – May 23, 2017.
[17] McPherson J. W. Reliability Physics and Engineering: Time-To-Failure Modeling. – Springer Science & Business Media, 2013. 399 p.
[18] Lorenz D. Aging Analysis of Digital Integrated Circuits: genehmigten Dissertation – Lehrstuhl f¨ur Entwurfsautomatisierung, Technischen Universit¨at Munchen – 2012.
[19] Drapatz S. Parametric Reliability of 6T-SRAM Core Cell Arrays : genehmigten Dissertation – Lehrstuhl f¨ur Technische Elektronik der Technischen Universit¨at M¨unchen – 2012.
[20] Massey, J.G. NBTI: What we know and what we need to know a tutorial addressing the currennt understanding and challenges for the future // IEEE International Integrated Reliability Workshop Final Report, 2004 - S. Lake Tahoe, CA, USA (Oct. 18-21, 2004).

Model for Detecting Counterfeit Recovered SRAMs Based on Accelerated Aging

V.N. Starcev, A.V. Semenov

«18 central research institute», Moscow, memory.test@ya.ru

***Abstract* — We considered new model for detecting recovered SRAM based on accelerated aging. The problem of detecting counterfeit recovered IC is difficult. A priori information required for decision making is not always available. Full reliability tests are lengthy and expensive. We studied the degradation model for SRAM. We have shown that using the SRAM degradation model based on NBTI allows us to get a rule for detecting restored chip. We have shown that accelerated aging methods for SRAM have a stable effect on the rate of change in the parameters of statistical distributions. The proposed model applied not only for SRAM. The model is also applicable for others integrated circuits (microcontrollers, FPGAs). At the same time, the required duration of stress effects can be calculated experimentally for various types of products.**

***Keywords* — counterfeiting, accelerated aging, NBTI, SRAM.**

REFERENCES

[1] ГОСТ Р 57880-2017. The system of protection against fraud and counterfeiting. Electronic products. Prevention of receipt, detection methods, reduction of application risks and decision on the use of counterfeit and counterfeit products [Text]. - Vved. 31-10-2017. - Moscow: Federal Agency for technical regulation and Metrology; Moscow: standardinform, 2017. (In Russian)
[2] Guin, U. et al. Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead // Journal of Electronic Testing. – February 2014.
[3] Arndt K. et al. Reliability of laser activated metal fuses in drams // Proc. of IEEE on Electronics Manufacturing Technology Symposium, 1999, pp. 389– 394.
[4] Robson N. et al. Electrically programmable fuse (efuse): From memory redundancy to autonomic chips // Proc. of IEEE on Custom Integrated Circuits Conference, 2007, pp. 799–804.
[5] Pappu, R. Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / R. Pappu // Massachusetts Institute of Technology (MIT). – Cambridge, 2001. – 154 p.
[6] Suh G., Devadas S. Physical unclonable functions for device authentication and secret key generation // Proc. of ACM/IEEE on Design Automation Conference, June 2007, pp. 9 –14.

[7] Kursawe K. et al. Reconfigurable physical unclonable functions - enabling technology for tamper-resistant storage // Proc. of IEEE International Workshop on Hardware-Oriented Security and Trust, July 2009, pp. 22 –29.
[8] Semenov A.V., Startsev V. N., Stepanov E.N. Technometric identification of integrated circuits for controlling life cycle and counterfeit detection / / problems of perspective micro- and nanoelectronic systems (MES). - 2018. - no. 4. - P. 143-148. (In Russian)
[9] Arkhipova I. V., Baturin A. V., Levin R. G., Mityushov A. I. Testing of methodology for reliability assessment of electronic components for fuse technology on the results of tests of small samples FPGA Altera. Voprosy radioelektroniki, 2017, no. 7, pp. 87–92. (In Russian)
[10] Pat. US 7592876 B2 USA, Int. Cl. HO3K 3/03, GOIR 3L/26. Leakage oscillator based aging monitor / Paul F. Newman ; Intel Corporation, Santa Clara, CA (US). – appl. №.:11/298,018 ; filed Dec. 8, 2005; date of Patent Sep. 22, 2009.
[11] Savanur P., Tragoudas S. A Method to Determine the Static NBTI Stress Time of Embedded Component in an Integreted Circuit // VALID 20176: The Ninth International Conference on Advances in System Testing and Validation.
[12] Pat. US 2017/O126229 A1 USA, Int. Cl. HO3K 9/003, HOIL 23/525, GOIR 3L/28, GITC 17/18. On-chip aging sensor and counterfeit integrated circuit detection method / Tan S. et al. ; Riverside, CA (US). – appl. №. 15/338,170, filed Oct. 28, 2016, Pub. Date May 4, 2017.
[13] Bhuvaneswari M. et al. Recycled IC Detection Based on AF and RO Sensors for Security and Reliability // International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Special Issue 6, May 2015 pp. 500-506.
[14] Pat. EP0623900A1, Int. Cl. G07C3/00. Recycable component with data storage for storing information for examining the component and product including such a component / Scheidt L. et al.; Sony International (Europe). – appl. №. EP0623900A1, filed 1994-11-09, Pub. Date 2004-03-10.
[15] Zhang X., Tehranipoor M. Design of On-chip Light-weight Sensors for Effective Detection of Recycled ICs // IEEE Transactions on VLSI (TVLSI), 2013.
[16] Gao Y., et al. Detecting Recycled Commodity SoCs: Exploiting Aging-Induced SRAM PUF Unreliability // Preprint submitted to Integration, The VLSI Journal. – May 23, 2017.
[17] McPherson J. W. Reliability Physics and Engineering: Time-To-Failure Modeling. – Springer Science & Business Media, 2013. 399 p.
[18] Lorenz D. Aging Analysis of Digital Integrated Circuits: genehmigten Dissertation – Lehrstuhl f¨ur Entwurfsautomatisierung, Technischen Universit¨at Munchen – 2012.
[19] Drapatz S. Parametric Reliability of 6T-SRAM Core Cell Arrays : genehmigten Dissertation – Lehrstuhl f¨ur Technische Elektronik der Technischen Universit¨at M¨unchen – 2012.
[20] Massey, J.G. NBTI: What we know and what we need to know a tutorial addressing the currennt understanding and challenges for the future // IEEE International Integrated Reliability Workshop Final Report, 2004 - S. Lake Tahoe, CA, USA (Oct. 18-21, 2004).