УДК 004.021+ 004.056.55+621.382.2:[621.315.592.3+620.192.63]

Дмитрий О. Петров[1], Виктор В. Буслюк[2], Станислав С. Дереченник[3],
Виктор А. Емельянов[4]
[1,2,3]Брестский государственный технический университет,
ул. Московская 267, Брест, 224017, Республика Беларусь
[2,4]ОАО «Цветотрон»,
ул. Суворова 96А, Брест, 224022, Республика Беларусь
[4]ОАО «Интеграл»,
ул. Казинца И.П., 121А, Минск, 220108, Республика Беларусь
[1]e-mail: polegdo@gmail.com, https://orcid.org/0000-0001-6164-9936
[2]e-mail: vbusliuk58@gmail.com, https://orcid.org/0000-0003-0090-3771
[3]e-mail: ssderechennik@gmail.com, https://orcid.org/0000-0001-9895-781X
[4]e-mail: emeljnov@bk.ru, https://orcid.org/0000-0002-9921-6682

ШУМОВЫЕ ДИОДЫ КАК ИСТОЧНИК ЭНТРОПИИ ДЛЯ АППАРАТНЫХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

DOI: http://dx.doi.org/10.26583/bit.2023.4.09

Аннотация. Целью настоящей статьи является анализ применения генераторов цифрового шума на основе полупроводниковых шумовых диодов в составе систем формирования ключевых числовых последовательностей, применяемых в методах криптографической защиты информации. Рассмотрена классификация современных методов криптографической защиты информации и лежащие в их основе алгоритмы. Показано, что обеспечение высокой информационной энтропии в системах порождения ключей шифрования возможно при использовании генераторов истинно случайных числовых последовательностей и криптографически стойких генераторов псевдослучайных числовых последовательностей. Описывается ряд недостатков присущих широко применяемым источникам физического шума: низкая спектральная плотность широкополосного шума, ограниченный диапазон частот, нелинейность спектра шума, сложности технической реализации, особенно в условиях крайних температур и воздействия специальных факторов. Подтверждено, что шумовые свойства полупроводниковых шумовых диодов зависят от состава и постоянства дефектно-примесной структуры, а инженерия дефектов позволяет управлять их электрическими параметрами. Исследование неоднородностей и дефектов шумовых диодов и разработка на этой основе способов управления уровнем структурных дефектов позволили создать технологии их генерации и отжига, улучшить ряд электрических и статистических свойств шумовых диодов.

Ключевые слова: криптография, криптографический алгоритм, энтропия, ключ шифрования, генератор цифрового шума, шумовой диод, инженерия дефектов, отжиг.

Для цитирования: ПЕТРОВ Дмитрий О. и др. ШУМОВЫЕ ДИОДЫ КАК ИСТОЧНИК ЭНТРОПИИ ДЛЯ АППАРАТНЫХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ. Безопасность информационных технологий, [S.l.], т. 30, № 4, с. 137–149, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1562. DOI: http://dx.doi.org/10.26583/bit.2023.4.09.

Dmitry O. Petrov[1], Viktor V. Busliuk[2], Stanislav S. Derechennik[3], Viktor A. Emeljanov[4]
[1,2,3]Brest State Technical University,
Moskovskaya str. 267, Brest, 224017, Belarus
[2,4]Tsvetotron, JSC,
Suvorova str. 96A, Brest, 224022, Belarus
[4]Integral, JSC,
Kazintsa I.P. str., 121A, Minsk, 220108, Belarus
[1]e-mail: polegdo@gmail.com, https://orcid.org/0000-0001-6164-9936
[2]e-mail: vbusliuk58@gmail.com, https://orcid.org/0000-0003-0090-3771
[3]e-mail: ssderechennik@gmail.com, https://orcid.org/0000-0001-9895-781X
[4]e-mail: emeljnov@bk.ru, https://orcid.org/0000-0002-9921-6682

Noise diodes as a source of entropy for hardware random number generators

DOI: http://dx.doi.org/10.26583/bit.2023.4.09

Abstract. The purpose of this article is to describe the use of digital noise generators based on semiconductor noise diodes as part of systems for generating key numerical sequences used in cryptographic security methods. The classification of modern methods of cryptographic protection and the algorithms underlying them are considered. It is shown that ensuring high information entropy in systems for generating encryption keys is possible by using generators of truly random number sequences and cryptographically secure generators of pseudo-random number sequences. A number of disadvantages inherent in widely used sources of physical noise are described, namely: low spectral density of broadband noise, limited frequency range, nonlinearity of the noise spectrum, difficulties in technical implementation when using some methods, especially under conditions of extreme temperatures and exposure to special factors. It has been confirmed that the noise properties of semiconductor noise diodes depend on the composition and constancy of the defect-impurity structure, and defect engineering makes it possible to control their electrical parameters. The study of inhomogeneities and defects in noise diodes and the development on this basis of methods for controlling the level of structural defects made it possible to create technologies for their generation and annealing, and to improve a number of electrical and statistical properties of noise diodes.

Keywords: Cryptography, cryptographic algorithm, entropy, encryption key, digital noise generator, noise diode, defect engineering, annealing.

For citation: PETROV Dmitry O. et al. Noise diodes as a source of entropy for hardware random number generators. IT Security (Russia), [S.l.], v. 30, no. 4, p. 137–149, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1562. DOI: http://dx.doi.org/10.26583/bit.2023.4.09.

Введение

В конце XIX века до формулирования Керкгхоффсом принципов построения криптографических систем и разработки теории информации Шенноном, одной из важных основ надежности защиты информации при помощи шифрования считалось сохранение в тайне применяемых криптографических алгоритмов [1, 2]. С развитием криптологии как науки на современном этапе, при размещении государственных стандартов по защите данных и соответствующих криптографических алгоритмов в открытом доступе, основой безопасности шифруемых данных является непредсказуемость формирования ключевой последовательности [2, 3]. Система, формирующая ключевую последовательность, должна характеризоваться высоким уровнем информационной энтропии [4] и на практике часто представляет собой генератор случайной числовой последовательности (ГСЧП) [5]. В свою очередь генераторы случайных числовых последовательностей можно подразделить на две категории: генераторы псевдослучайных числовых последовательностей (ГПСЧП) и генераторы истинно случайных числовых последовательностей (ГИСЧП). В основе генераторов псевдослучайных числовых последовательностей лежат детерминированные итерационные алгоритмы, принимающие в качестве входных данных некоторое начальное число и выдающие на выходе периодически повторяющуюся последовательность чисел [1, 6, 7]. Генераторы истинно случайных последовательностей чисел представляют собой устройства, измеряющие параметры непредсказуемых физических процессов, являющимися источниками энтропии и преобразующие их в случайный битовый поток. В качестве источников энтропии, используемых в генераторах истинно случайных числовых последовательностей можно привести, например, тепловой шум Джонсона–Найквиста [8], природный радиационный фон [9], квантово-механические процессы [10], свойства лавинного пробоя *p-n* перехода диода [11, 12]

1. Современные методы криптографической защиты информации

В настоящее время используемые методы криптографической защиты информации можно разбить на две основные категории – симметричные с секретным ключом и ассиметричные с открытым ключом [1, 13, 14]. Алгоритмы, лежащие в основе симметричных методов криптографической защиты информации, подразумевают использование одной и той же секретной ключевой последовательности как для шифрования данных передающей стороной, так и для дешифрования принимающей стороной. Ассиметричные методы криптографической защиты (криптосистемы с открытым ключом) информации используют алгоритмы, применяющие для шифрования несекретный открытый ключ, а для дешифрования используется секретный закрытый ключ, известный только получателю зашифрованной информации.

По способу обращения с потоком данных симметричные алгоритмы шифрования с секретным ключом можно подразделить на блочные и поточные – первые обрабатывают поступающий поток данных группами (блоками) бит длина которых нередко кратна машинному слову используемого при выполнении вычислений микропроцессора, а вторые обрабатывают битовый поток данных [13].

Среди блочных шифров следует отметить отличающиеся своей актуальностью шифр AES (Advanced Encryption Standard) с размером блока 128 бит и размером ключа, выбираемом из ряда 128, 192 и 256 бит, а также группу шифров ГОСТ 34.12-2018 с размером ключа 256 бит с размерами блока 64 бита и 128 бит. Шифр AES является государственным стандартом шифрования США с 2002 г. [14], а группа шифров ГОСТ 28147-89 [1] является национальным стандартом РФ с 2019 г.

Поточные шифры имеют преимущество перед блочными шифрами по скорости шифрования и при этом тесно связаны с генераторами псевдослучайных числовых последовательностей. К генераторам псевдослучайных последовательностей, применяемым в поточных шифрах, предъявляются следующие требования: генерируемая последовательность чисел должна быть статистически неотличима от абсолютно случайной за небольшое время вычислений и знание какой-либо части последовательности не должно позволять предсказать следующий элемент этой последовательности за небольшое время вычислений [1].

Достаточно известными поточными шифрами являются шифр RC4 с рекомендуемой длиной ключа от 128 бит и выше, широко использовавшиеся в криптографических протоколах передачи данных SSL и TLS и семейство шифров A5 с длиной ключа 64 бита, применяемых для шифрования оцифрованного речевого сигнала в стандарте мобильной связи GSM [13, 14, 15].

Криптостойкость ассиметричных методов шифрования основана на вычислительной сложности некоторых математических задач – например, безопасность шифра RSA основана на трудоемкости факторизации больших целых чисел разрядностью более 2048 бит, а для систем шифрования на эллиптических кривых стойкость к криптоанализу основана на сложности выполнения операции дискретного логарифмирования на эллиптической кривой [1, 13, 14].

[1] ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. URL: https://docs.cntd.ru/document/1200161708 (дата обращения: 20.10.2023).

2. Генераторы псевдослучайных числовых последовательностей

В общем случае генераторы псевдослучайных числовых последовательностей можно представить как функцию *F(s, i)* где s – начальное число, а i – порядковый номер генерируемого двоичного слова заданной разрядности [1]. Для иллюстрации принципа работы ГПСЧП можно привести линейный конгруэнтный генератор, итерационно выполняющий вычисления по формуле

$$x_{i+1} = (ax_i + b)\ mod\ c,$$

где a, b и c – некоторые предварительно выбранные константы, а в качестве начального числа используется значение x_0 [1, 7].

Примером ГПСЧП с возможностью аппаратной реализации является использование регистра сдвига с линейной обратной связью (РСЛОС). Обратная связь в этом случае представляет собой операцию логического сложения по модулю 2 над некоторыми битами регистра (рис. 1) [7, 13]. В качестве входных данных РСЛОС принимает начальное число в двоичной системе счисления, а выходными данными является последовательность битов.

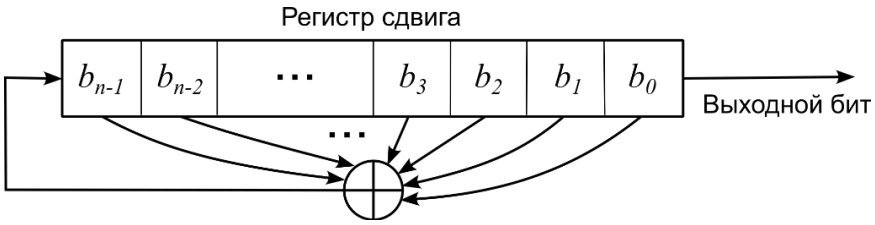

Рис. 1. Регистр сдвига с линейной обратной связью
Fig. 1. Structure of linear feedback shift register

Значительная часть известных реализаций ГПСЧП непригодны для использования в криптографии по причине предсказуемости для криптоаналитика генерируемых ими последовательностей чисел [16]. Отдельную группу среди ГПСЧП составляют криптостойкие генераторы псевдослучайных числовых последовательностей (КГПСЧП) – генерируемая ими последовательность чисел статистически неотличима от абсолютно случайной за небольшое время вычислений и знание какой-либо части последовательности не позволяет предсказать следующий элемент этой последовательности за небольшое время вычислений [1, 7]. Например, в качестве криптостойких генераторов псевдослучайных чисел могут быть использованы известные блоковые шифры, работающие в режиме обратной связи по выходу OFB (Output Feed Back) [1].

3. Генераторы истинно случайных числовых последовательностей

Общая структура ГИСПЧ приведена на рис. 2 [7]. На структурной схеме источник энтропии представляет собой модуль, измеряющий некоторый характерные параметры непредсказуемого физического процесса и преобразующий его в форму электрического сигнала. Электрический сигнал от источника энтропии поступает в модуль оцифровки, но так как получаемые после оцифровки сигнала логические нули и единицы могут быть неравновероятны или зависят друг от друга, то их последовательность поступает в модуль обработки цифрового сигнала для преобразования в равновероятную и независимую [1]. Преобразованная последовательность битов может либо напрямую поступать на выход ГИСЧП, либо использоваться в качестве начального значения генератора псевдослучайной числовой последовательности в зависимости от архитектуры ГИСЧП [7, 11].

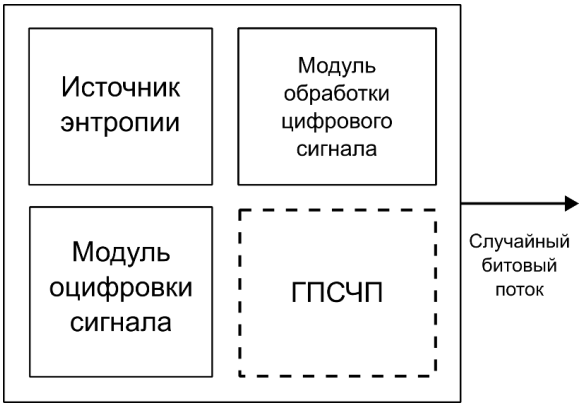

Рис. 2. Общая структура генераторов истинно случайных числовых последовательностей
Fig. 2. General structure of truly random number sequence generators

4. Шумовые диоды в составе генераторов истинно случайных числовых последовательностей

В связи с дискретностью энергетических уровней носителей зарядов и неизбежностью электрических флуктуаций, создаваемых ими при определенных условиях, с учетом миниатюризации приборов полупроводниковые источники физического шума (диоды-генераторы шума, лавинно-пролетные диоды, стабилитроны) в настоящее время находят все более широкое применение. Благодаря ряду потребительских преимуществ, таких как небольшие габариты, малые напряжения питания (менее 10 В), а также приемлемые величины спектральной плотности, специально разработанные и выпускаемые рядом отечественных и зарубежных фирм шумовые диоды (ШД), кроме того, обладают преимуществом как источники физического шума для оценки качества приемо-передающих устройств и цифровых каналов передачи информации, маскирования побочных электромагнитных излучений, а также, как отмечено выше, для генерации криптографически случайных числовых последовательностей в аппаратно-программных комплексах защиты информации. На рис. 3 приведена типовая электрическая схема генератора цифрового шума на базе шумового диода для использования в составе ГИСЧП.

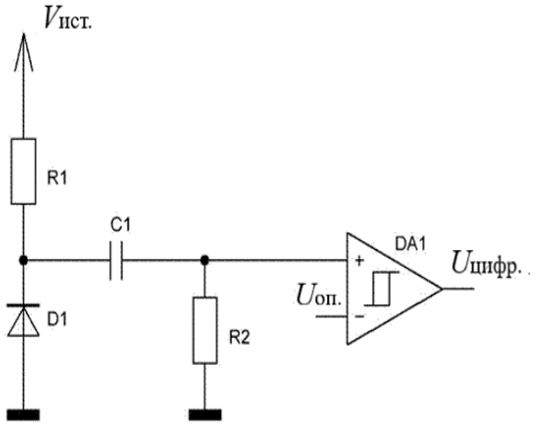

Рис. 3. Схема электрическая принципиальная генератора цифрового шума
Fig. 3. Electrical circuit diagram of a digital noise generator

Согласно техническим условиям на ШД, параметр «постоянное напряжение шумового диода» определяет напряжение электрического пробоя обратносмещенного

p-*n*-перехода ШД. В реальных схемах шумовых генераторов, напряжение пробоя шумового диода *D*1 достигается за счет падения напряжения на токозадающем резисторе *R*1.

5. Новые направления совершенствование технологии производства шумовых диодов

Причинами шума ШД являются микроплазменные образования в области пространственного заряда (ОПЗ) диодов, зависящие от наличия неоднородностей структуры, дефектов, а также характера переноса тока в коротких ОПЗ. Так как напряжение лавинного пробоя большинства шумовых диодов находится в диапазоне 6–9 В, то для их создания требуются высоколегированные кремниевые структуры, для которых фактический разброс их основных электрофизических параметров значительно выше, чем для слаболегированных. Это накладывает дополнительные требования на качество исходных подложек по стабильным характеристикам уровня легирования, содержания кислорода, углерода и плотности дефектов. Таким образом, воспроизводимость электрофизических параметров шумовых диодов зависит от множества конструктивно-технологических факторов, в том числе от концентрации основных примесей и примесей чужеродных элементов, наличия и концентрации неоднородностей и несовершенств кристаллической решетки, вакансионно-кислородных комплексов, динамики процессов преципитации и геттерирования, а также от применяемых технологических режимов легирования и отжига структур [17].

Актуальным для потребителей ШД является увеличение интенсивности генерации бинарного сигнала при расширении диапазона задаваемых токов, расширение температурного диапазона применения, сохранение электрофизических свойств ШД при воздействии специальных факторов. Актуальным для производителей ШД является изучение влияния неоднородностей и дефектов на их электрофизические параметры и разработка на этой основе способов управления уровнем структурных дефектов высоколегированных кремниевых структур для улучшения электрических и статистических свойств ШД, а также применение радиационных технологических методов для целенаправленного изменения этих свойств. Такие задачи относятся к новому направлению микроэлектроники – инженерии дефектов.

В ходе работ по совершенствованию ШД серий ND101–104, ND201 и 2Г103А9, на основе анализа ВФХ и ВАХ в режимах прямого и обратного включения при положительных и отрицательных температурах, с учетом масс-спектров ВИМС установлены виды дефектов в структурах ШД, преимущественно влияющих на их шумовые свойства. На рис. 4 представлены графики зависимостей энергии активации от приложенного напряжения. Путем экстраполяции к оси ординат при U = 0 В получены глубины залегания энергетических уровней вторичных примесей, которые находятся в диапазоне 0,45±0,03 эВ. Такие значения энергии позволяют идентифицировать наличие фоновых технологических примесей меди и железа, ионизация которых, в том числе, приводит к возникновению микроплазменного шума (рис. 5) [18].

Анализ данных, полученных на масс-анализаторе TOF.SIM 5, позволяет предположительно установить основные технологические операции, в ходе которых вторичные металлы попадают в структуру ШД. Как показано в [18], примесь меди сконцентрирована в зоне *p*-*n*-переходов ШД, в том числе, в высоколегированной области охранного кольца. В связи с этим следует предположить, что основной источник вторичных атомов железа и меди – высокотемпературные процессы формирования *p*-*n*-переходов ШД методом диффузии. Основной источник этих металлов – промывные воды, используемые на операциях отмывки. Контроль химического состава

деионизированной воды, а также поддержание ее постоянного удельного сопротивления может гарантировать постоянство содержания вторичных металлов. Установление конкретных значений физико-химических параметров деионизированной воды, используемой на этих технологических операциях для производства ШД, требует дополнительных исследований. Однако такой подход создаст дополнительные трудности в массовом производстве ШД. Проблема может быть решена путем запуска в производство партий ШД с конкретным содержанием меди и железа в исходных пластинах (например, с концентрацией по верхнему пределу технических условий 1×10^{11} см$^{-3}$). При этом необходимо обеспечить соответствующее качество деионизированной воды на всех этапах технологического процесса.

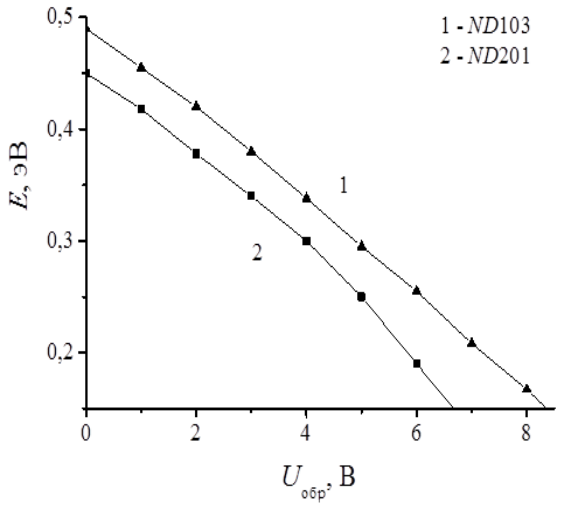

Рис. 4. Зависимость энергии активации от обратного напряжения
Fig. 4. Dependence of activation energy on reverse voltage

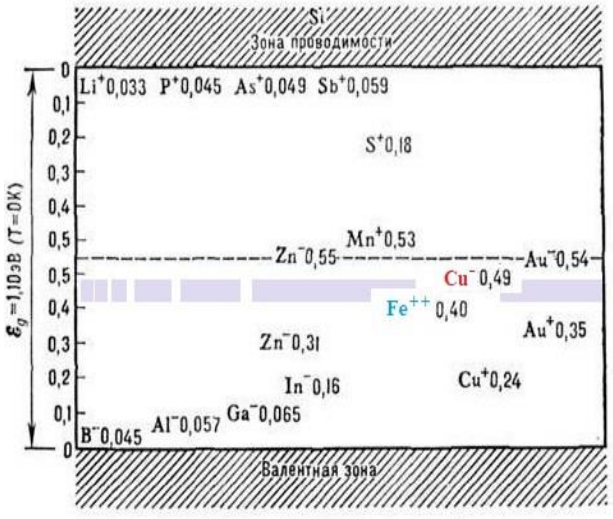

Рис. 5. Уровни энергий примесей в кремнии
Fig. 5. Energy levels of impurities in silicon

Для управления дефектообразованием предложена технология создания дефектов в полупроводниковых кремниевых пластинах оптимальной кристаллографической ориентации, используемых для ШД [19, 20]. Сущность данной технологии состоит в том, что стабильная дислокационная структура в зоне *p*-*n*-перехода достигается эффективным управлением распределения неконтролируемых примесей. Процесс оплавления локальных зон производится с обратной стороны пластин кремния (111) или (001) с помощью лазерного пучка с длиной волны 1,064 мкм и мощностью порядка 100 Вт с последующим высокотемпературным отжигом при окислении и прорастанием дислокаций на планарную сторону пластины. Равномерное их распределение по объему *p*-*n*-перехода кристалла обеспечивается за счет сформированных дефектов структуры с образованием Si_3N_4.

Установлено, что наибольшего выхода годных ШД можно достичь при выполнении параллельных зон оплавления шириной d = (10–100) мкм с шагом a = (1,5…5,0)×d, в одном из двух основных типов кристаллографических направлений – ⟨112⟩ или ⟨110⟩ с последующей делокализацией дислокационной структуры в активную область при температуре 1200°C в течение не менее 2,5 ч. На рис. 6 представлена предложенная схема расположения механических нарушений на нерабочей поверхности пластины ориентации

(001) по отношению к кристаллографическим направлениям. На рис. 7 – расположение нерегулярной сетки дислокаций, декорированной ионами кальция.

Принципы формирования дислокаций: использование основных плоскостей скольжения дислокаций в кремнии – {111} и {110}; оптимизация дефектообразования за счет управления направлениями роста (для (111) – тип ⟨112⟩, для (001) – тип ⟨110⟩; веерообразное распространение дислокаций при отжиге. Формирование дислокаций в других направлениях приводит к их пересечению на некотором расстоянии и блокируется вследствие образования полупетель. Обеспечение стабильности и равномерности дефектов в зоне *p*-*n*-перехода ШД за счет предложенной технологии позволяет увеличить на 3–5% выход годных изделий по сравнению с образцами, неподвергнутыми воздействию лазера.

Разработана технология герметизации и отжига готовых полупроводниковых структур и кристаллов ШД [21]. В сильнолегированных структурах при отжиге в диапазоне температур 450–600°С происходит рост концентрации термодоноров кислорода, азота и межузельных атомов кремния. Значительное содержание ионов кислорода в области *p*-*n*-перехода кристалла позволяет констатировать, что в результате отжига происходит внутреннее геттерирование остаточных точечных дефектов и дислокаций на преципитатах SiOx.

В табл. 1. представлены результаты расчета числовых характеристик выборок измерений по каждому анализируемому параметру до и после отжига.

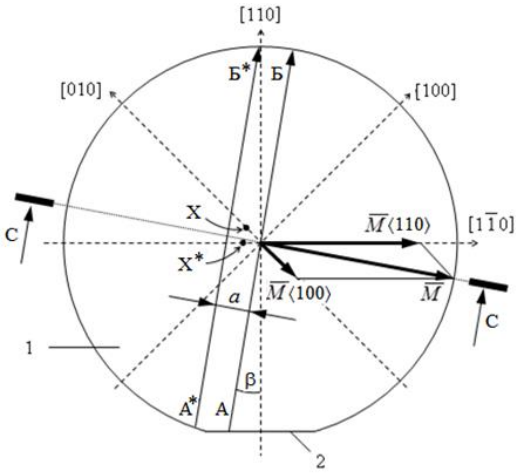

Рис. 6. Схема расположения механических нарушений на нерабочей поверхности пластины ориентации (001) по отношению к кристаллографическим направлениям:1-пластина, 2-базовый срез
Fig. 6. Diagram of the location of mechanical disturbances on the non-working surface of the orientation plate (001) in relation to the crystallographic directions: 1-plate, 2-base slice

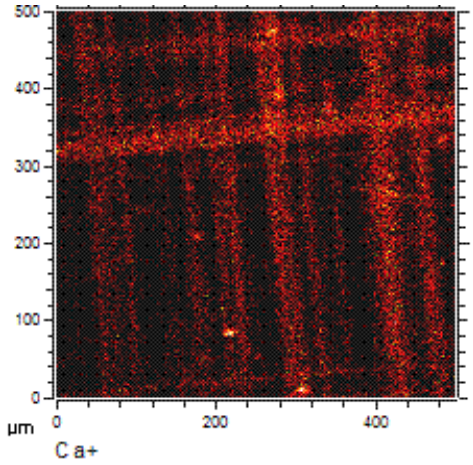

Рис. 7. Нерегулярная сетка дислокаций, декорированная ионами кальция
Fig. 7. Irregular network of dislocations decorated with calcium ions

Таблица 1. Значения числовых характеристик случайных параметров ШД ND103 до и после отжига

Режим измерений	Названия и обозначения числовых характеристик для выборок измерений случайных параметров						Существенные изменения характеристик
	минимум (min)	максимум (max)	размах (R)	среднее (m)	с.к.о. (б)	медиана (Me)	
Для выборки измерений спектральной плотности напряжения шума S_U, мкВ/Гц $^{1/2}$							
до отжига (кристаллы)	34	72	38	56,6	7,26	55	рост: m Su – на 9,9 %; снижение: б Su – на 34 %, R Su – на 34,2 %
после отжига (ДГШ)	52	77	25	62,2	5,52	64	
Для выборки измерений нелинейности спектральной плотности напряжения шума δS_U, дБ							
до отжига (кристаллы)	1,37	1,95	0,58	1,70	0,147	1,72	снижение: m δSu – на 42,9 %, б δSu – на 23 %, R δSu – на 25,9 %
после отжига (ДГШ)	0,78	1,21	0,43	0,97	0,113	0,96	
Для выборки измерений граничной частоты шумового сигнала $f_{гр}$, МГц							
до отжига (кристаллы)	3,08	5,03	1,95	3,72	0,345	3,76	снижение: m $f_{гр}$– на 35,5 %, б $f_{гр}$ – на 17,8 %, R $f_{гр}$ – на 34,9 %
после отжига (ДГШ)	1,76	3,03	1,27	2,40	0,283	2,39	
Для выборки измерений эффективного напряжения шума Uэф, мВ							
до отжига (кристаллы)	101	168	67	141,8	12,18	140,0	снижение: m Uэф – на 6,1 %, б Uэф–на 35,3 %, R Uэф – на 61,2 %
после отжига (ДГШ)	122	148	26	133,1	7,88	132,5	

В ходе исследований показано, что отжиг кристаллов и готовых ШД на финишных операциях при времени отжига (80 ± 3) мин в температурном диапазоне 450–600°С с нагревом со скоростью 4–7°С/мин, изотермической стадией в течение (19 ± 1) мин и охлаждением со скоростью 3,8–5,0°С/мин, является эффективным методом стабилизации шумовых параметров и обеспечивает повышение спектральной плотности шума и значительное (более чем в 1,7 раза) снижение ее неравномерности. Важнейшим результатом этого отжига является снижение разброса значений исследуемых параметров шума: по $U_{эф}$ – на 61,2%, по S_U – на 34,2%, по $f_{гр}$ – на 34,9%, по δS_U – на 25,9% [22, 23]. Это позволяет улучшить качество случайных числовых последовательностей в программно-аппаратных комплексах защиты информации.

Предложенные технологии апробированы в производстве ШД и аналого-цифровых шумовых модулей на их основе. Для оценки качества ШД были разработаны и реализованы измерительные схемы и алгоритмы цифровой обработки шумовых сигналов. Это подтвердило состоятельность разработанных технологических методов как для дискретных ШД, так и для аналого-цифровых шумовых модулей [24]. Оценку энтропии последовательности импульсов шумового сигнала до и после внедрения новых методов

создания и стабилизации дефектов производили путем расчета и сравнения фактора Фано (ФФ) по методике, изложенной в [25]. При этом после внедрения получены значения ФФ близкие к 1, а энтропия для диодов ND103 при перенапряжении 0,15 В составила 0,999999, что подтвердило близость генерируемой последовательности к пуассоновскому потоку [26].

Исследования выполнены с использованием вторично-ионной масс-спектроскопии, оптической микроскопии, стандартных методик измерения электрических и тепловых характеристик полупроводниковых приборов. Измерения ВАХ и ВФХ диодов с целью определения влияния генерационных центров на электрофизические параметры ШД производились с помощью измерителя параметров полупроводниковых приборов Agilent B1500A (Agilent Technologies, США) и зондовой станции Cascade Summit 11000 (Cascade Microtech, США) в интервале температур от минус 60 до +125°С. Структурные дефекты подложки выявлялись путем травления в селективном хромовом травителе. Фактическое наличие примесных атомов в структуре ШД ND 103L исследовалось масс-спектрометром TOF.SIMS 5 (IONTOF, Германия). Отжиг структур производился в печи PP 40/85 (Sokol-Therm, Deutschland GmbH) в среде азота одновременно с герметизацией кристаллов в металлостеклянный корпус. При этом использовался стеклокапилляр JD38(CIT, Ireland Ltd, Great Britain).

Заключение

Рассмотрены преимущества использования генераторов цифрового шума на основе шумовых диодов в качестве источника энтропии генераторов истинно случайных числовых последовательностей. В ходе исследований установлены виды дефектов структуры и закономерности их образования, преимущественно влияющие на электрические и статистические параметры кремниевых ШД. Показано, что лавинный пробой *p*-*n*-переходов ШД серий ND101−104, ND 201, а также 2Г103А9 обеспечивается в значительной мере локальными неоднородностями легирования подложки, а также электрической ионизацией глубоких примесных центров технологических (фоновых) примесей меди и железа. Предложен новый способ изготовления полупроводниковой кремниевой пластины ориентаций (111) и (001), обеспечивающий создание устойчивого уровня дефектности сильнолегированных слоев кремния, используемого для производства ШД.

Оптимизация процесса дефектообразования в структуре достигается за счет направленного роста дислокаций под воздействием излучения лазера непрерывного действия ($Y_3Al_5O_{12}$, длина волны 1,064 мкм) путем сканирования с обратной стороны пластины в азотной среде. Последующий термический отжиг обеспечивает релаксацию механических напряжений и делокализацию дислокационной структуры в активную область *p*-*n*-перехода. Минимальная длина получаемых при этом дислокаций, а также термическая стабильность включений Si_3N_4 в зонах оплавления предопределяет дальнейшую устойчивость дислокаций к воздействию различных технологических факторов.

Предложены и реализованы технологические режимы совмещенного с герметизацией кристаллов отжига высоколегированных структур ШД. В реализованных условиях отжига в присутствии технологических примесей кислорода и азота увеличивается концентрация термодоноров, что приводит к формированию устойчивых преципитатов кремния с кислородом. Преципитаты являются эффективными геттерами технологических примесей и способствуют стабилизации дефектно-примесного ансамбля высоколегированных структур. Этим обеспечивается улучшение параметров ШД: сужение диапазона разброса средних значений основных электрических параметров, рост спектральной плотности напряжения шума при снижении ее неравномерности.

СПИСОК ЛИТЕРАТУРЫ:

1. Рябко Б.Я. Криптографические методы защиты информации: учебное пособие. М.: Горячая линия-Телеком, 2017. – 230 с. ISBN 978-5-9912-0286-2.
2. Vassilev A., Hall T.A. The Importance of Entropy to Information Security. Computer. 2014, vol. 47, no. 2, p. 78–81. DOI: http://dx.doi.org/10.1109/MC.2014.47.
3. Van Herrewege A., Van der Leest V., Schaller A., Katzenbeisser S., Verbauwhede I. Secure PRNG Seeding on Commercial Off-the-Shelf Microcontrollers. TrustED '13: Proceedings of the 3rd international workshop on Trustworthy embedded devices. 2013, p. 55–64. DOI: https://doi.org/10.1145/2517300.2517306.
4. Аверин Г.В., Звягинцева А.В. О взаимосвязи статистической и информационной энтропии при описании состояний сложных систем. Прикладная математика & Физика. 2016, № 20(241). URL: https://cyberleninka.ru/article/n/o-vzaimosvyazi-statisticheskoy-i-informatsionnoy-entropii-pri-opisanii-sostoyaniy-slozhnyh-sistem (дата обращения: 20.10.2023).
5. Афанасенков А.С., Кучинский П.В., Новик М.И., Петрунин П.Ю., Ращеня Н.А. Аппаратно-программное устройство генерации случайных числовых последовательностей с USB-интерфейсом. Комплексная защита информации: Материалы XXI научно-практической конференции, Смоленск. 2016, с. 70–74.
6. Григорьев А.Ю. Методы тестирования генераторов случайных и псевдослучайных последовательностей. Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2017, № 1, с. 22–28. – EDN YSUQMX.
7. Cao Y., Liu W., Qin L., Liu B., Chen S., Ye J., Xia X., Wang C. Entropy Sources Based on Silicon Chips: True Random Number Generator and Physical Unclonable Function. Entropy. 2022, 24(11):1566. DOI: https://doi.org/10.3390/e24111566.
8. Jun B., Kocher P. The Intel® random number generator. Cryptography Research Inc. White Paper, San Francisco. 1999. URL: https://www.semanticscholar.org/paper/The-intel-random-number-generator-Jun-Kocher/6dd9928f4704f49151624a030491c514133471a9 (дата обращения: 20.11.2023).
9. Багров К.В., Рычкова А.А. Разработка метода генерации случайных чисел на основе природного радиационного фона. Символ науки. 2021, № 6. URL: https://cyberleninka.ru/article/n/razrabotka-metoda-generatsii-sluchaynyh-chisel-na-osnove-prirodnogo-radiatsionnogo-fona (дата обращения: 20.10.2023).
10. Balygin K.A., Zaitsev V.I., Klimov A.N., Kulik S.P., Molotkov S.N., Popova E., Vinogradov S. Quantum random number generator based on ‘Fermi–Dirac’ statistics of photocounts of faint laser pulses with a 75 Mbit s^{-1} rate. Laser Phys. Lett. 2017, 14 125207. DOI: https://doi.org/10.1088/1612-202X/aa930e.
11. Mandana Ewert. 2018. A Random Number Generator Based on Electronic Noise and the Xorshift Algorithm. In Proceedings of the 2018 VII International Conference on Network, Communication and Computing (ICNCC '18). Association for Computing Machinery, New York, NY, USA, 357–362. DOI: https://doi.org/10.1145/3301326.3301359.
12. Горбадей О.Ю., Зеневич А.О. Использование диодов-генераторов шума для создания двухуровневой случайной числовой последовательности. Телекомунікаційні та інформаційні технології. 2017, № 3(56), с. 12–17. – EDN YNNGFV.
13. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Издательство ТРИУМФ, 2003. – 816 с. ISBN 5-89392-055-4.
14. Авдошин С.М., Савельева А.А. Криптографические методы защиты информационных систем. Известия АИН им. А.М. Прохорова. Бизнес-информатика. 2006, т. 17, с. 91–99. URL: https://www.hse.ru/data/005/621/1235/001.pdf?ysclid=lp9o1i8ra5238827399 (дата обращения: 20.11.2023).
15. Орлов В.Г., Мазуркевич Д.О. Алгоритмы шифрования в публичных беспроводных сетях. T-Comm. 2011, № 10. URL: https://cyberleninka.ru/article/n/algoritmy-shifrovaniya-v-publichnyh-besprovodnyh-setyah (дата обращения: 20.10.2023).
16. Будько М.Б., Будько М.Ю., Гирик А.В., Грозов В.А. Методы генерации и тестирования случайных последовательностей. СПб: Университет ИТМО, 2019. – 70 с.
17. Буслюк В.В. Шумовые полупроводниковые диоды с управляемым уровнем дефектности высоколегированных кремниевых структур. Автореферат диссертации на соискание ученой степени кандидата технических наук. Минск. БГУИР, 2022. URL: http://dep.nlb.by/jspui/handle/nlb/57451 (дата обращения: 20.10.2023).
18. Buslyuk, V.V., Odzhayev, V.B., Panfilenko, A.K. et al. Physical Parameters of the Broadband Noise-Generator Diodes. Russ Microelectron. 2020, no. 49, p. 295–301. DOI: https://doi.org/10.1134/S1063739720040034.
19. Емельянов В.В., Емельянов В.А., Сенько С.Ф., Буслюк В.В., Просолович В.С., Дереченник С.С. Способ изготовления полупроводниковой кремниевой пластины ориентации (001): пат. BY 22406 C2. – Опубл. 30.12.2018.

20. Емельянов В.В., Емельянов В.А., Сенько С.Ф., Буслюк В.В., Просолович В.С., Дереченник С.С. Способ изготовления полупроводниковой кремниевой пластины ориентации (111): пат BY 22465 C2. – Опубл. 30.12.2018.
21. Буслюк В.В. Технология кремниевых диодов генераторов шума. Электроника, наука, технология, бизнес. № 4 (205), 2021, с. 136–138.
22. Емельянов В.В. и др. Формирование стабильной дефектной структуры в кремниевых диодах генераторов шума. Вести НАН Беларуси. Сер. физ.-техн. наук. 2021, т. 66, № 2. DOI: https://doi.org/10.29235/1561-8358-2021-66-2-145-153.
23. Буслюк В.В., Емельянов В.А., Баранов В.В., Дереченник С.С., Просолович В.С. Стабилизация шумовых параметров при отжиге высоколегированных структур диодов – генераторов шума. Доклады БГУИР. 2021, т. 19(6), с. 32–41. DOI: http://dx.doi.org/10.35596/1729-7648-2021-19-6-32-41.
24. Разумейчик В.С. и др. Оценка вероятностных характеристик случайных сигналов микроэлектронного шумового модуля. Вестник Брестского государственного технического университета. Физика, Математика, Информатика. 2014, № 5(89), с. 41–45. – EDN YUMKYP.
25. Барановский О.К., Кучинский П.В., Чернявский А.Ф. Вести НАН Беларуси. Сер. физ.-мат. наук. 2004, № 4, с. 105–110. Оценка энтропии случайных числовых последовательностей, формируемых с использованием физического источника шума.
26. Барановский О. К., Горбадей О.Ю., Зеневич А.О., Сильченко О.М. Исследование возможности использования шумовых диодов для генерации пуассоновского потока импульсов. Проблемы инфокоммуникаций. 2017, № 1 (5), с. 13–18.

REFERENCES:

[1] Ryabko B.Ya. Cryptographic methods of information protection: textbook. M.: Hotline-Telecom, 2017. – 230 p. ISBN 978-5-9912-0286-2 (in Russian).
[2] Vassilev A., Hall T.A. The Importance of Entropy to Information Security. Computer. 2014, vol. 47, no. 2, p. 78–81. DOI: http://dx.doi.org/10.1109/MC.2014.47.
[3] Van Herrewege A., Van der Leest V., Schaller A., Katzenbeisser S., Verbauwhede I. Secure PRNG Seeding on Commercial Off-the-Shelf Microcontrollers. TrustED '13: Proceedings of the 3rd international workshop on Trustworthy embedded devices. 2013, p. 55–64. DOI: https://doi.org/10.1145/2517300.2517306.
[4] Averin G.V., Zviagintseva A.V. The statistical and information entropy relationship when describing the complex systems state. Applied Mathematics & Physics. 2016, no. 20(241). URL: https://cyberleninka.ru/article/n/o-vzaimosvyazi-statisticheskoy-i-informatsionnoy-entropii-pri-opisanii-sostoyaniy-slozhnyh-sistem (accessed: 20.10.2023) (in Russian).
[5] Afanasenkov A.S., Kuchinsky P.V., Novik M.I., Petrunin P.Yu., Raschenya N.A. Hardware-software device for generating random numerical sequences with a USB interface. Complex information protection: Materials of the XXI scientific and practical conference, Smolensk. 2016, p. 70–74 (in Russian).
[6] Grigoriev A.Yu. Methods of testing generators of random and pseudorandom sequences. Scientific notes of USU. Ser. Mathematics and information technology. UlSU. Electron. Journal. 2017, no. 1, p. 22–28 (in Russian). – EDN YSUQMX.
[7] Cao Y., Liu W., Qin L., Liu B., Chen S., Ye J., Xia X., Wang C. Entropy Sources Based on Silicon Chips: True Random Number Generator and Physical Unclonable Function. Entropy. 2022, 24(11):1566. DOI: https://doi.org/10.3390/e24111566.
[8] Jun B., Kocher P. The Intel® random number generator. Cryptography Research Inc. White Paper, San Francisco. 1999. URL: https://www.semanticscholar.org/paper/The-intel-random-number-generator-Jun-Kocher/6dd9928f4704f49151624a030491c514133471a9 (accessed: 20.10.2023).
[9] Bagrov K.V., Rychkova A.A. Development of a method for generating random numbers based on natural radiation background. A symbol of science. 2021, no. 6. URL: https://cyberleninka.ru/article/n/razrabotka-metoda-generatsii-sluchaynyh-chisel-na-osnove-prirodnogo-radiatsionnogo-fona (accessed: 20.10.2023) (in Russian).
[10] Balygin K.A., Zaitsev V.I., Klimov A.N., Kulik S.P., Molotkov S.N., Popova E., Vinogradov S. Quantum random number generator based on ‘Fermi–Dirac’ statistics of photocounts of faint laser pulses with a 75 Mbit s^{-1} rate. Laser Phys. Lett. 2017, 14 125207. DOI: https://doi.org/10.1088/1612-202X/aa930e.
[11] Mandana Ewert. 2018. A Random Number Generator Based on Electronic Noise and the Xorshift Algorithm. In Proceedings of the 2018 VII International Conference on Network, Communication and Computing (ICNCC '18). Association for Computing Machinery, New York, NY, USA, 357–362. DOI: https://doi.org/10.1145/3301326.3301359.

[12] Gorbadey O. Yu., Zenevich A. A. Use of the diodes-noise generators to create a two-level random numerical sequence. 2017, no. 3(56), p. 12–17 (in Russian). – EDN YNNGFV.
[13] Schneier B. Applied Cryptography. Protocols, algorithms, source texts in C. M.: TRIUMPH Publishing House, 2003. – 816 p. ISBN 5-89392-055-4 (in Russian).
[14] Avdoshin S.M., Savelyeva A.A. Cryptographic methods of information systems protection. Izvestia of the A.M. Prokhorov Institute. Business informatics. 2006, vol. 17, p. 91–99. URL: https://www.hse.ru/data/005/621/1235/001.pdf?ysclid=lp9o1i8ra5238827399 (дата обращения: 20.10.2023) (in Russian).
[15] Orlov V.G., Mazurkevich D.O. Encryption algorithms in public wireless networks. T-Comm. 2011, no. 10. URL: https://cyberleninka.ru/article/n/algoritmy-shifrovaniya-v-publichnyh-besprovodnyh-setyah (accessed: 20.10.2023) (in Russian).
[16] Budko M.B., Budko M.Yu., Girik A.V., Grozov V.A. Methods of generating and testing random sequences. St. Petersburg: ITMO University, 2019. – 70 p. (in Russian).
[17] Buslyuk V.V. Noise semiconductor diodes with a controlled level of defectiveness of high-alloyed silicon structures. Abstract of the dissertation for the degree of Candidate of Technical Sciences. Minsk. BGUIR, 2022. URL: http://dep.nlb.by/jspui/handle/nlb/57451 (accessed:20.10.2023).
[18] Buslyuk, V.V., Odzhayev, V.B., Panfilenko, A.K. et al. Physical Parameters of the Broadband Noise-Generator Diodes. Russ Microelectron. 2020, no. 49, p. 295–301. DOI: https://doi.org/10.1134/S1063739720040034.
[19] Emelyanov V.V., Emelyanov VA., Senko S. F, Buslyuk VV., Prosolovich V.S., Derechennik S.S. Method of manufacturing a semiconductor silicon wafer orientation (001): pat. BY 22406 C2. – Publ. 30.12.2018 (in Russian).
[20] Emelyanov V.V., Emelyanov V.A., Senko S.F., Buslyuk V.V., Prosolovich V.S., Derechennik S.S. Method of manufacturing a semiconductor silicon wafer orientation (111): pat BY 22465 C2. – Publ. 12/30/2018 (in Russian).
[21] Buslyuk V.V. Technology of silicon diodes-noise generators. Electronics, science, technology, business. No. 4(205), 2021, p. 136–138 (in Russian).
[22] Emelyanov V.V. et al. Formation of a stable defects structure in silicon noise diodes. Vestsi Natsyyanal'nai akademii navuk Belarusi. Seryya fizika-technichnych navuk = Proceedings of the National Academy of Sciences of Belarus. Physical-technical series. 2021, vol. 66, no. 2, p. 145–153. DOI: https://doi.org/10.29235/1561-8358-2021-66-2-145-153 (in Russian).
[23] Busliuk V.V., Emelyanov V.A., Baranov V.V., Derechennik S.S., Prasalovich V.S. Stabilization of noise parameters during annealing of highly alloyed structures of noise diodes. Doklady BGUIR. 2021;19(6):32-41. DOI: https://doi.org/10.35596/1729-7648-2021-19-6-32-41 (in Russian).
[24] Razumeychik V. S. et al. Estimation of probabilistic characteristics of random signals of a microelectronic noise module. Bulletin of the Brest State Technical University. Physics, Mathematics, Computer Science. 2014, no. 5(89), p. 41–45 (in Russian). – EDN YUMKYP.
[25] Baranovskij O.K., Kuchinskij P.V., Chernyavskij A.F. Estimating the entropy of random numerical sequences generated using a physical noise source. Vesti NAN Belarusi. Ser. fiz.-mat. nauk. 2004, no. 4, p. 105–110 (in Russian).
[26] Baranovskij O.K., Gorbadej O.Yu., Zenevich A.O., Sil`chenko O.M. Study of the possibility of using noise diodes to generate a Poisson pulse stream. Problemy` infokommunikaczij. 2017, no 1 (5), p. 13–18 (in Russian).

Поступила в редакцию – 21 октября 2023 г. Окончательный вариант – 25 ноября 2023 г.
Received – October 21, 2023. The final version – November 25, 2023.