УДК 621.377.6, 621.3.049.77

Особенности применения методов помехоустойчивого кодирования в суб–100-нм микросхемах памяти для космических систем

А.А. Краснюк[1,2], К.А. Петров[2]

[1]Национальный исследовательский ядерный университет «МИФИ», Москва, aakrasnyuk@mephi.ru

[2]ФГБУН НИИ Системных Исследований РАН, Москва

***Аннотация* — Рассмотрены основные и перспективные методы коррекции кратных ошибок на основе помехоустойчивого кодирования по Хэммингу в суб-100-нм микросхемах памяти, находящихся под воздействием одиночных и дозовых радиационных факторов.**

***Ключевые слова* — статическая оперативная память (СОЗУ), одиночные и дозовые радиационные эффекты, устойчивость к сбоям, помехоустойчивое кодирование, коды Хэмминга.**

I. Введение

Высокопроизводительные вычислительные системы на основе суб-100-нм проектных норм в настоящее время востребованы различными отраслями: от ядерной энергетики и радиационной медицины до авиационно–космических систем и экстремальной электроники. Хотя данные проектные нормы и позволяют реализовать на кристалле устройства, содержащие десятки миллионов транзисторов, наличие в конструкции транзисторов приборных слоев с толщинами 1,5-5 нм делает данные схемы чрезвычайно чувствительными к одиночным и дозовым радиационным эффектам, как показано на рис. 1 [1]. В частности, при переходе к суб-100-нм проектным нормам становится практически невозможным спроектировать ячейки и регистры статической оперативной памяти (СОЗУ) микропроцессоров таким образом, чтобы они выдерживали внешнюю атаку ионизирующих частиц [2]. До 50% отказов в современном оборудовании, работающем в условиях воздействия внешней радиации, так или иначе связаны с влиянием дозовых и однократных радиационных эффектов именно на элементы памяти. Кроме того, суб-100-м технологии, как правило, являются уникальными и чрезвычайно специализированными, поэтому возможности их модернизации в плане повышения радиационной стойкости технологическими и конструктивными мерами практически отсутствуют. По этим причинам в последние годы сформировалось значимое научное направление развития методов радиационной стойкости для суб-100-нм электронных систем исключительно средствами схемотехнического и алгоритмического проектирования – Radiation Hardening by Design – RHBD.

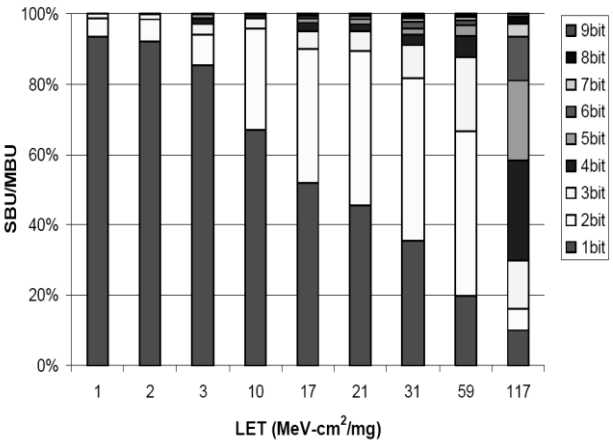

Рис. 1. Отношение одиночных (SBU) и мультибитных сбоев (MBU) в коммерческой 90-нм КМОП СБИС ОЗУ в зависимости от линейных потерь энергии ОЯЧ (LET)

Как показали проведенные исследования, для суб-100-нм СОЗУ наибольшую эффективность обеспечивает именно сочетание современных схемотехнических решений для элементов памяти и алгоритмических методов кодирования и защиты данных, которое позволяет не только обеспечивать минимизацию вероятности сбоя, но и возможность исправления уже произошедших ошибок [3]. Если решение вопросов исправления однократных ошибок отработано на субмикронных СБИС ОЗУ, то коррекция и исправление кратных ошибок для суб-100-нм СБИС, обеспечивающия сохранение быстродействия, является актуальной и востребованной задачей. В статье проводится анализ возможности коррекции кратных ошибок на основе кодов, исправляющих смежные двукратные ошибки, а

также представлены коды собственной разработки, исправляющие смежные двукратные ошибки.

II. Типы помехоустойчивых кодов

Большинство ошибок в элементах и микросхемах памяти, относится к одиночным ошибкам. Однако для суб-100-нм схем практически все сбои данных, обусловленные одиночными радиационными эффектами, становятся парными и кратными [4]. Это связано с существенно меньшими размерами ячеек памяти в сравнении с размерами треков ионизирующих частиц в объеме кристалла микросхемы. Разнесение и перемежение данных в разряде слова на кристалле микросхемы позволяет частично уменьшить данный эффект [5]. Тем не менее на рис. 1 проиллюстрирована ситуация возникновения двукратной смежной ошибки в кодовом слове по адресу 4 при воздействии отдельной ядерной частицы даже при использовании метода перемежения данных в массиве памяти. Поэтому, де-факто встроенное помехоустойчивое кодирование, обеспечивающее обнаружение и исправление как минимум парных ошибок, становится обязательной опцией при разработке современных микросхем памяти и встроенных СОЗУ для радиационно-стойких применений.

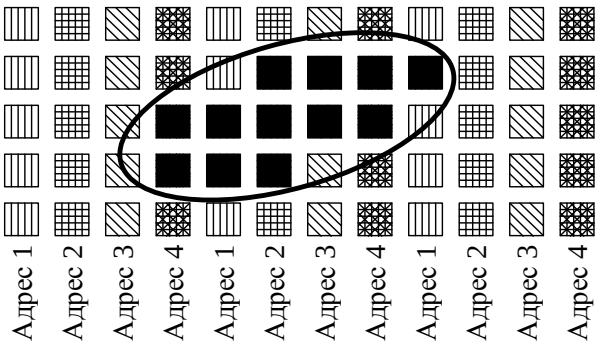

Рис. 2. Двукратная смежная ошибка (адрес 4) при перемежении данных в массиве памяти

Необходимо определить эффективность различных подходов к решению данной задачи. Среди помехоустойчивых кодов существуют несколько типов, используемых для различных целей. Наиболее эффективным типом кодов для борьбы со сбоями в СОЗУ при сохранении высокого быстродействия и малой аппаратной избыточности является тип линейных блочных кодов Хэмминга [6].

Рассмотрим линейные блочные SEC-DED (single-error-detection double-error-correction) коды типа Хэмминга, позволяющие исправлять однократные и детектировать двукратные ошибки в кодовом слове. Каждый код типа Хэмминга однозначно определяется соответствующей ему проверочной H-матрицей. В соответствии с H-матрицей происходит вычисление проверочных битов при записи кодового слова в СОЗУ и детектирование ошибки при чтении и декодировании кодового слова. При декодировании каждый столбец H-матрицы соответствует синдрому, означающему ошибку в бите, номер которого совпадает с номером столбца. В случае многократной ошибки суммарный синдром будет представлять собой результат побитового сложения по модулю два тех столбцов H-матрицы, номера которых совпадают с номерами ошибочных битов.

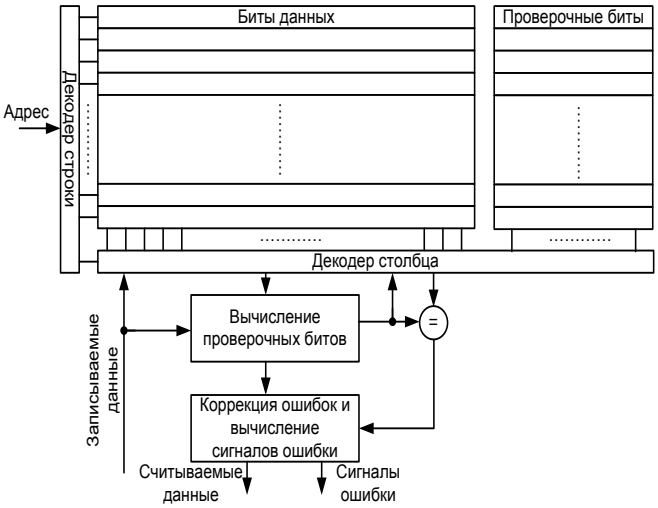

Рис. 3. Функциональная схема использования помехоустойчивого кодирования в СБИС ОЗУ

При проектировании элементов памяти (пример функциональной схемы приведен на рис. 3) наиболее распространенные размерности информационных слов (16, 32, 64 и т.д.) не являются оптимальными для кодов, вследствие чего возникает избыточность, выражающаяся в том, что SEC-DED код может детектировать часть ошибок кратности больше двух. Эту избыточность можно также использовать для исправления двукратных смежных ошибок, преобразовав уже существующий SEC-DED код в SEC-DAEC (double-adjacent-error-correction) код. Для этого столбцы проверочной матрицы SEC-DED кода необходимо переставить так, чтобы суммарные синдромы ошибок в любых двух смежных битах не совпадали друг с другом.

При использовании SEC-DAEC кода существует вероятность неправильного исправления несмежных двукратных ошибок, синдромы которых совпадают с синдромами смежных двукратных ошибок. Одним из основных критериев, по которым оцениваются SEC-DAEC коды, является процент неверного исправления несмежных двукратных ошибок. Чем эта цифра меньше, тем более устойчивым к сбоям является код.

На рис. 4 приведена функциональная схема разработанного декодера для SEC-DAEC кода, которая отличается от стандартной схемы декодера SEC-DED кода наличием дополнительного генератора вектора ошибки – в данном случае двукратной смежной, а также более сложным генератором сигналов наличия ошибки, когда необходимо анализировать большее количество векторов ошибки.

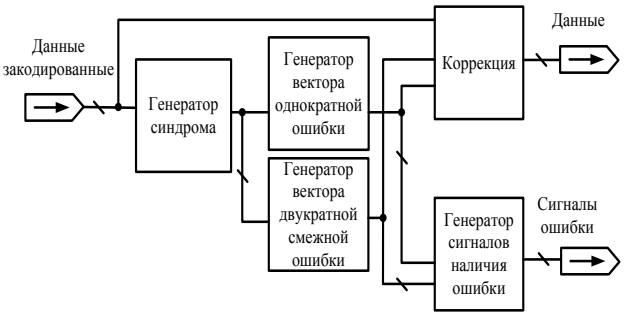

Рис. 4. Декодер SEC-DAEC кода

При перестановке столбцов проверочной матрицы кода определяется их порядок. Нахождение определенного порядка столбцов может быть сделано с помощью различных методов: как полного перебора всех возможных вариантов, так и с помощью эвристических алгоритмов, когда возможных вариантов слишком много. К таким SEC-DAEC кодам относятся коды Дутта [7] и коды Ричтера [8]..

III. Моделирование и анализ результатов

На основании проверочных матриц кодов для 32- и 64-разрядного информационных слов было проведено моделирование с помощью специально разработанного прикладного ПО CheckMatrix. Также с использованием генетических алгоритмов [9] были получены коды, превосходящие коды Ричтера по количеству правильно детектируемых двукратных несмежных ошибок. На основании проверочных матриц полученных кодов также было проведено моделирование, и результаты представлены для анализа.

Был проведен сравнительный анализ среди SEC-DAEC кодов. Анализ проводился по трем критериям: аппаратная избыточность, характеризуемая количеством 2-входовых элементов «исключающее-ИЛИ» в кодере; быстродействие, характеризуемое максимальным количеством единиц в строке проверочной матрицы; устойчивость к сбоям, характеризуемая вероятностью ошибочной коррекции двукратных ошибок.

Сравнительные характеристики кодов Дутта, Ричтера и предложенного кода для 32- и 64-разрядных информационных слов представлены в табл. 1.

По результатам сравнительного анализа предложенный код обладает наилучшей устойчивостью к сбоям (детектирует до 27% больше несмежных двукратных ошибок) при худших характеристиках быстродействия и занимаемой площади на кристалле.

Также среди рассмотренных схемотехнических решений повышения устойчивости элементов памяти к сбоям был определен метод дополнительных столбцов [9].

Метод заключается в том, что при проектировании схем памяти в массив вводятся дополнительные столбцы и мультиплексоры, позволяющие при возникновении многократных сбоев в каком либо столбце заменять его дополнительным. Этот схемотехнический метод можно дополнить алгоритмическим: дополнительные столбцы, пока они не используются для замены, можно использовать для хранения дополнительных проверочных битов кодового слова, внеся соответствующие изменения в кодер и декодер. К кодам с дополнительными проверочными битами относятся коды Датта [10] и коды Чоя [11].

Таблица 1

Сравнительные характеристики SEC-DAEC кодов

Код	Кол-во 2-входовых элементов «Исключающее ИЛИ»	Максимальное кол-во единиц в строке проверочной матрицы	Вероятность ошибочной коррекции двукратных ошибок, %
Дутта (39, 32)	96	15	53,4
Ричтер (39, 32)	115	20	38,6
Предложенный код (39, 32)	130	20	35,5
Дутта (72, 64)	224	32	53
Ричтер (72, 64)	250	37	34,8
Предложенный код (72, 64)	284	39	33,8

Было проведено сравнительное моделирование кодов Датта, Чоя и предложенного кода. Результаты анализа полученных в ходе моделирования характеристик кодов представлены в табл. 2 – для 32-разрядного информационного слова, и в табл. 3 – для 64-разрядного информационного слова.

Таблица 2

Сравнительные характеристики SEC-DAEC кодов для 32-разрядного информационного слова, использующих дополнительные проверочные биты

Код	Кол-во 2-входовых элементов «Исключающее ИЛИ»	Максимальное кол-во единиц в строке проверочной матрицы	Вероятность ошибочной коррекции двукратных ошибок, %
Датта (40, 32)	117	16	27,4
Чоя (40, 32)	134	18	10,1
Предложенный код (40, 32)	147	20	6,9
Датта (41, 32)	130	16	13,8
Чоя (41, 32)	162	19	2,9
Предложенный код (41, 32)	155	21	0,3
Датта (42, 32)	140	15	8,8
Чоя (42, 32)	166	21	2
Предложенный код (42, 32)	194	20	0

По результатам сравнительного анализа определено, что предложенный код обладает наилучшей устойчивостью к сбоям (детектирует до 20% больше несмежных двукратных ошибок) при худших характеристиках быстродействия и занимаемой площади на кристалле. Для всех вариантов предложенного кода, а также кодов Дутта, Датта и Чоя были разработаны и исследованы RTL-модели на языке Verilog.

Таблица 3

Сравнительные характеристики SEC-DAEC кодов для 64-разрядного информационного слова, использующих дополнительные проверочные биты

Код	Кол-во 2-входовых элементов ИСКЛ-ИЛИ	Максимальное кол-во единиц в строке проверочной матрицы	Вероятность ошибочной коррекции двукратных ошибок, %
Датта (73, 64)	263	31	26,9
Чоя (73, 64)	294	34	15,8
Предложенный код (73, 64)	322	39	10,3
Датта (74, 64)	306	32	17,8
Чоя (74, 64)	311	33	6,4
Предложенный код (74, 64)	360	39	2,3
Датта (75, 64)	353	32	14,6
Чоя (75, 64)	358	38	2,2
Предложенный код (75, 64)	398	39	0,2

Необходимо отметить, что традиционные подходы к встроенным кодерам и декодерам помехоустойчивого кодирования не предусматривают различия в конструкции ячеек памяти для основного массива данных и проверочных (контрольных) битов. Это приводит к тому, что множественное поражение области проверочных битов приводит к катастрофическим потерям данных.

Поэтому полагаем оправданным применение различных схемотехнических решений для ячеек основной памяти и схем помехоустойчивого контроля, например, на ячейках памяти DICE (Dual Interlocked Storage Cell). Это позволяет до 10 раз уменьшить вероятность потери данных в области проверочных битов при воздействии протонами с энергией до 1 ГэВ [12].

IV. Заключение

Было проведено моделирование различных помехоустойчивых кодов, применяемых для исправления двукратных смежных ошибок в СОЗУ. Также предложен оригинальный помехоустойчивый код. По результатам сравнительного анализа предложенный код обладает наилучшей устойчивостью к сбоям (детектирует до 27% больше несмежных двукратных ошибок) при несколько худших характеристиках быстродействия и занимаемой площади на кристалле. Для всех вариантов предложенного кода, а также кодов Датта и Чоя были разработаны и исследованы RTL-модели на языке Verilog. Предложенные коды могут эффективно использоваться при детектировании и коррекции двукратных смежных ошибок в элементах памяти суб-100-нм микропроцессорных систем.

Литература

[1] Philippe Roche, Reno Harboe-Sorensen. Radiation Evaluation of ST Test Structures in commercial 130nm CMOS BULK and SOI; In commercial 90nm CMOS BULK; in commercial 65nm CMOS BULK and SOI // Final Presentation of ESTEC Contract No. 13528/95/NL/MV, COO-18; Progress Presentation of ESTEC Contract No. 18799/04/NL/AG, COO-3. STMicroelectronics. 2007. P. 30-31.

[2] Riaz Naseer. A framework for soft error tolerant sram design // A Dissertation presented to the faculty of the graduate school university of southern california. 2008. P. 134.

[3] Rim K. et al. Characteristics and device design of sub-100 nm strained Si N- and PMOSFETs // Symposium on VLSI Technology'02. June 2002. P. 98.

[2] International Technology Roadmap for Semiconductors 2007.www.itrs.net/links/2007itrs/2007_chapters/2007_PIDS.pdf.

[3] Satoh S. Geometric effect of multiple-bit soft errors induced by cosmic rayneutrons on DRAM // Electron Device Letters, IEEE. Jun 2000. Vol. 21. Issue 6. P. 310-312.

[4] Hung L.D. Soft-error tolerant cash architectures // Department of Information Science and Technology. The University of Tokyo. 2006. P. 41.

[5] Петров К.А. Особенности помехоустойчивого кодирования информации в ОЗУ // Электроника, микро- и наноэлектроника. Сборник научных трудов / под ред. В.Я. Стенина. М.: НИЯУ МИФИ, 2010. С. 167-172.

[6] Dutta A., Touba N.A. Multiple Bit Upset Tolerant Memory Using a Selective Cycle Avoidance Based SEC-DED-DAEC Code // 25th IEEE VLSI Test Symposium. 2007. P. 349-354.

[7] Richter M. and all. New Linear SEC-DED Codes with Reduced Triple Bit Error Miscorrection Probability // 14th Int. On-Line Testing Symposium. 2008. P 37-40.

[8] Holland J.H. Adaptation in natural and artificial systems. University of Michigan Press, Ann Arbor. 1975.

[9] Kim, I., and all. Built in self repair for embedded high density SRAM // Proc. of International Test Conf. 1998. P. 1112-1119.

[10] Datta R., Touba N.A. Exploiting Unused Spare Columns to Improve Memory ECC // VLSI Test Symposium. 2009. P. 47-52.

[11] Choi J.S. and all. SEC-DED-DAEC code for reducing miscorrection rate of double adjacent error // School of Electrical and Electronic Engineering. Yonsei University. 2010. P. 79-83.

[12] Стенин В.Я., Черкасов И.Г., Чумаков А.И., Яненко А.В. Исследование тестовых субмикронных КМОП статических ОЗУ на сбоеустойчивых ячейках памяти к эффектам воздействия протонов с энергией 1 ГЭВ // Радиационная стойкость электронных систем. Научно-техн. сборник. М.: МИФИ, 2009. Вып. 12. С. 77-78.