ИСПОЛЬЗОВАНИЕ СФОКУСИРОВАННОГО ЛАЗЕРНОГО ИЗЛУЧЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ СОСТОЯНИЯ ЯЧЕЕК ПАМЯТИ КМОП ОЗУ

Скоробогатов С.П.[1], *Скоробогатов П.К.*[2]

[1]Кембриджский университет,
[2]Московский инженерно-физический институт
(государственный университет)

Приведены результаты экспериментальных исследований и численного моделирования воздействия сфокусированного лазерного излучения на матрицу ячеек памяти КМОП ОЗУ, подтверждающие возможность определения таким способом состояния ячеек памяти.

Традиционные методы чтения содержимого защищенного ОЗУ основаны на использовании механических зондов, подключаемых к шинам обмена информацией [1,2]. Помимо чисто технических трудностей при использовании микропробников в современных БИС, применение таких методов может быть заблокировано встроенными аппаратными средствами защиты информации. Более эффективными являются методы, основанные на бесконтактном воздействии с использованием лазерного излучения (ЛИ) [3] и локального нестационарного магнитного поля [4].

С целью проверки эффективности оптических методов чтения информации из КМОП ОЗУ было выполнено лазерное сканирование области оперативной памяти микроконтроллера PIC16F84. Каждая из ячеек памяти контроллера представляет собой классическую 6-транзисторную КМОП ячейку, схема и топология которой приведены на рис.1.

В качестве источника ЛИ использовался непрерывный лазер с длиной волны 0,65 мкм, достаточной для ионизации кремния. Излучение фокусировалось с помощью микроскопа до диаметра около 1 мкм на поверхности кристалла. Исследуемый кристалл размещался на координатном столе и перемещался в направлениях

X и Y с шагом 0,1 мкм. В процессе сканирования измерялись значения тока по цепи питания ИС.

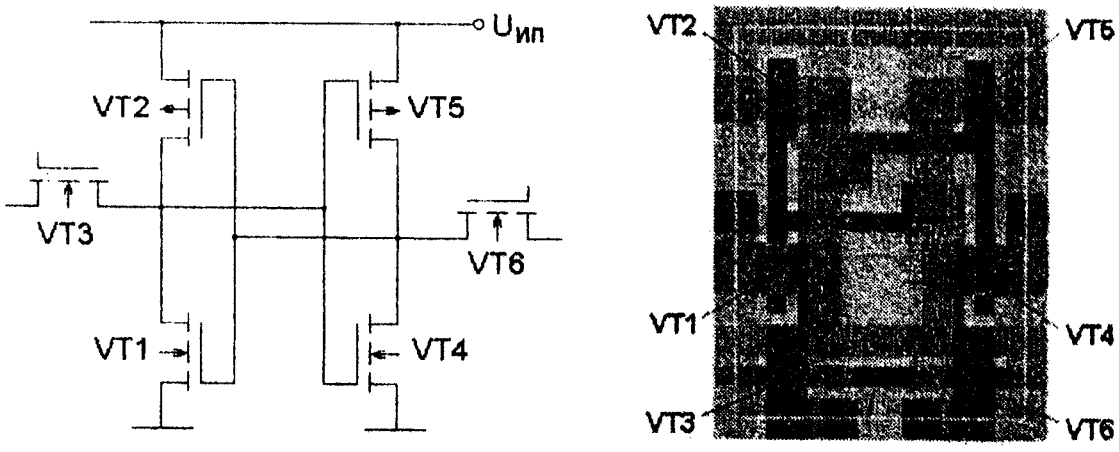


Рис.1. Схема и топология ячейки памяти КМОП ОЗУ

На рис.2 приведены результаты сканирования поверхности КМОП ОЗУ микроконтроллера при напряжении питания 2,5 В.

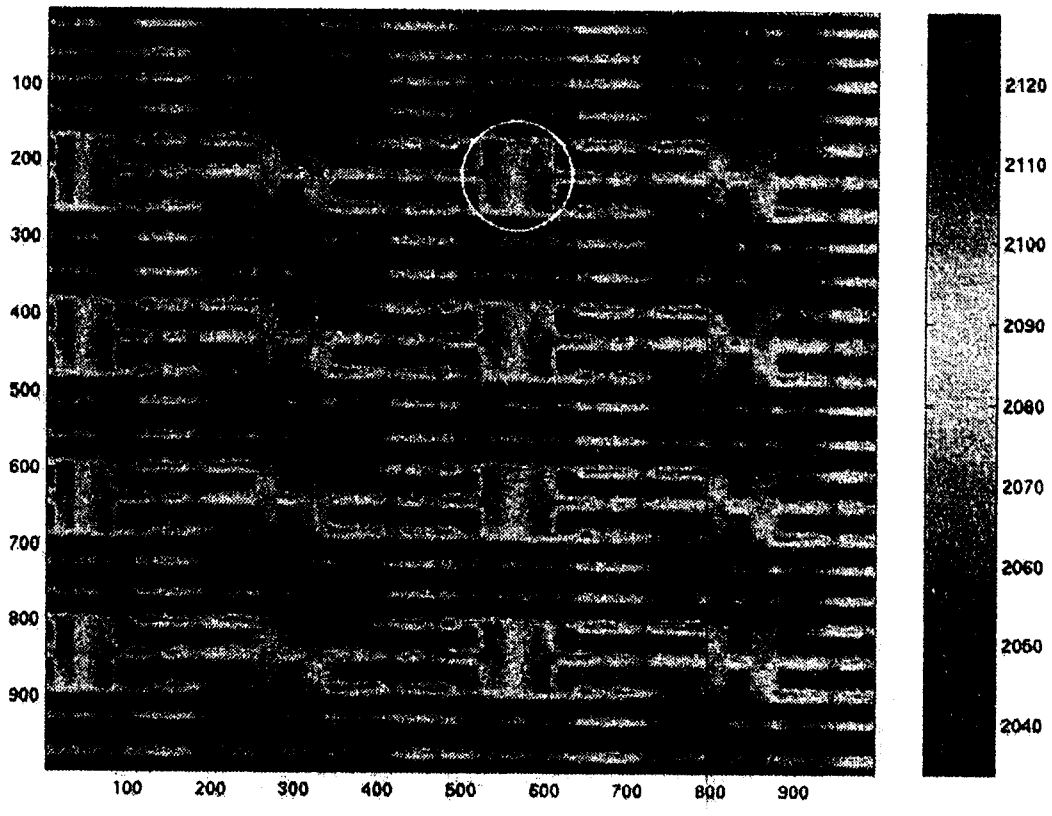


Рис.2. Результаты лазерного сканирования поверхности КМОП ОЗУ

Как и следовало ожидать, наибольший фотоотклик имеет место при локализации лазерного луча в районе областей стока и истока p- и n-канальных транзисторов ячеек памяти. Области с низким уровнем тока соответствуют областям металлизации, не пропускающим ЛИ. Результаты сканирования указывают также на заметное отличие в величине фотоотклика открытого и закрытого инверторов ячеек памяти (см. область внутри окружности на рис.2). Это различие может быть использовано для определения состояния ячеек памяти.

С целью интерпретации полученных результатов было выполнено численное двумерное моделирование ионизационной реакции КМОП-инвертора под действием сфокусированного ЛИ с использованием пакета "DIODE-2D" [5]. Поперечное сечение моделируемой структуры приведено на рис.3,а. Длина каналов транзисторов принималась равной 1 мкм, а интенсивность ЛИ - 10^4Вт/см^2.

Результаты расчета зависимостей тока цепи питания инвертора от местоположения лазерного луча, полученные для трех длин волн излучения и двух состояний инвертора, приведены на рис.3,б. Видно, что облучение области закрытого транзистора приводит к протеканию более высокого уровня тока в цепи питания, чем при облучении открытого. Связано это с тем, что канал открытого транзистора открывает путь для протекания фототока стока смежного (закрытого) транзистора через источник питания. Дополнительный вклад в этот эффект вносит также модуляция проводимости канала закрытого транзистора, увеличивая общий ток через структуру.

Обращает на себя внимание увеличение разности фотоотклика транзисторов инвертора в разных состояниях при уменьшении длины волны ЛИ. Этот эффект связан с уменьшением маскирующего действия фототока перехода карман-подложка вследствие роста коэффициента поглощения излучения и локализации ионизации преимущественно у поверхности структуры.

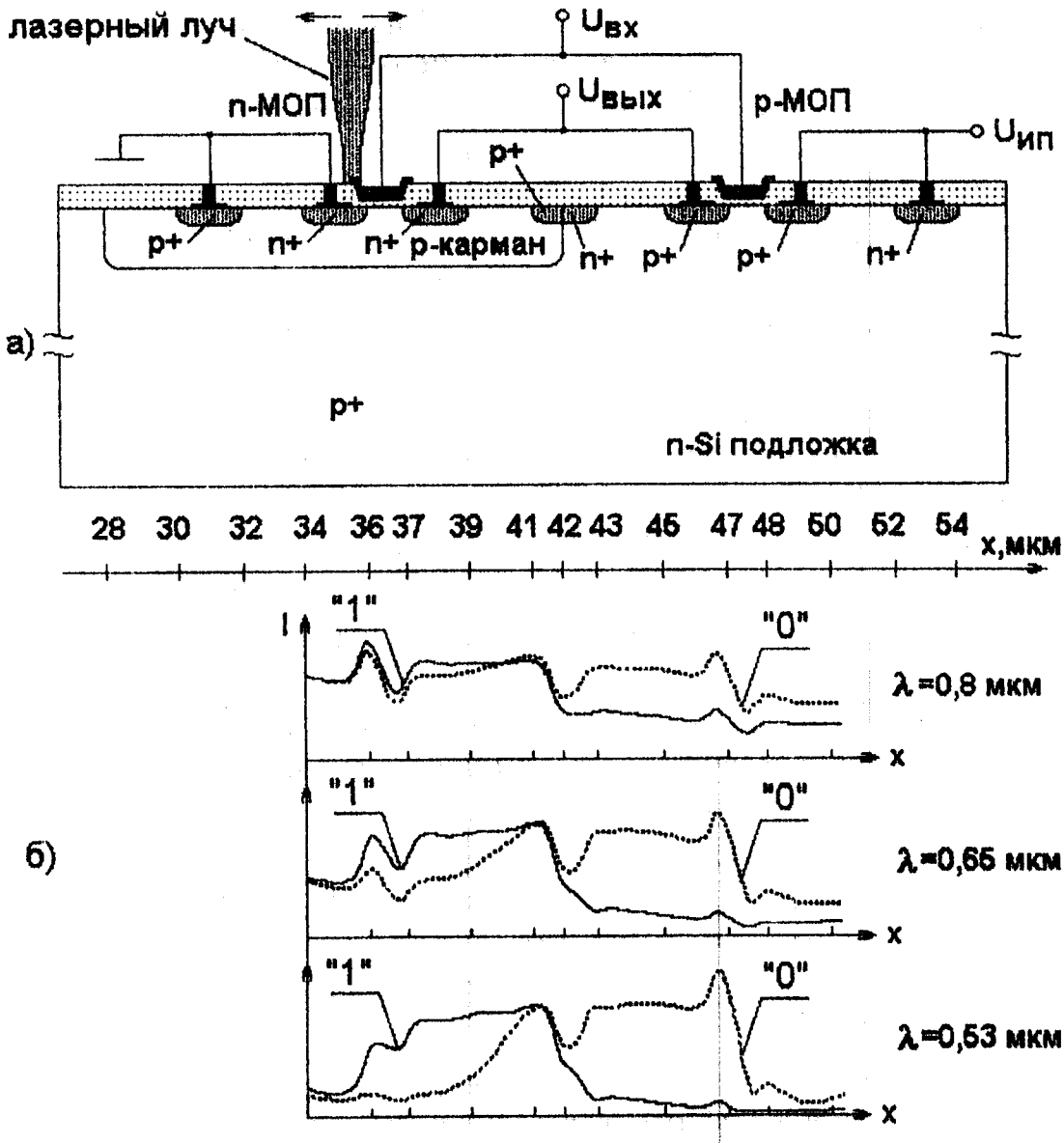
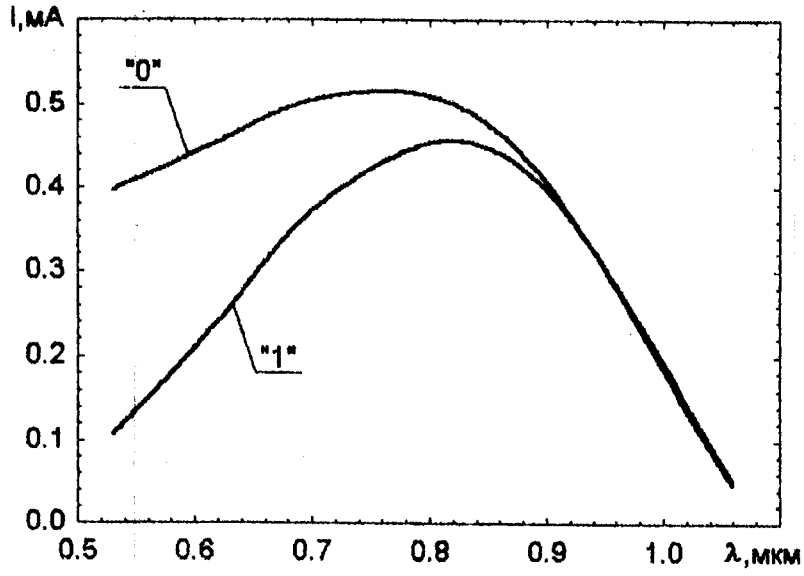
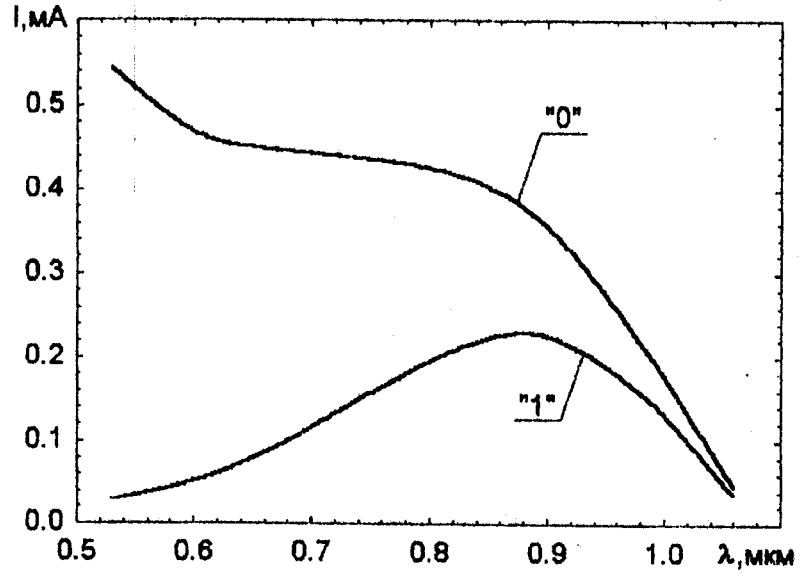


Рис.3. Поперечное сечение моделируемой структуры (а) и зависимости тока цепи питания КМОП-инвертора от местоположения лазерного луча для трех длин волн излучения и двух состояний инвертора (б)

Вывод о повышении эффективности метода при переходе на более короткие длины волн подтверждают результаты расчетов зависимостей токов цепи питания КМОП-инвертора от длины волны ЛИ, приведенные на рис.4. Чем короче длина волны, тем больше разность токов инвертора в зависимости от логического состояния.



а)



б)

Рис.4. Зависимости тока цепи питания КМОП-инвертора в двух состояниях от длины волны лазерного излучения при облучении области канала p-МОП транзистора (а) и n-МОП транзистора (б)

Подобное поведение наблюдалось и экспериментально: если при длине волны 0,65 мкм удавалось уверенно фиксировать разницу в состояниях транзисторов по току цепи питания, то при

переходе на длину волны 0,8 мкм – разность была на уровне шумов. Основным источником шума является фототок перехода карман-подложка, величина которого меняется при сканировании вдоль поверхности в зависимости от наличия или отсутствия в данном месте поликремниевых шин, стоковых или истоковых областей, уровня их легирования. Переход на более короткую длину волны ЛИ уменьшает вклад этих факторов.

Таким образом, результаты расчетов и экспериментов подтверждают возможность использования сфокусированного лазерного облучения для бесконтактного определения состояния ячеек памяти КМОП ОЗУ. С целью повышения надежности определения состояния ячеек следует использовать ЛИ с более короткими длинами волн.

Литература

1. Anderson R.J., Kuhn M.G. Tamper Resistance – a Cautionary Note // Proc. of the Second Usenix Workshop on Electronic Commerce, Nov., 1996. - P.1-11. http://www.cl.cam.ac.uk/users/rja14/tamper.html.
2. Kommerling O., Kuhn M.G. Design Principles for Tamper-Resistant Security Processors//Usenix Workshop on Smartcard Technology, 1999. http://www.cl.cam.ac.uk/Research/Security/Tamper/.
3. Skorobogatov S.P., Anderson R.J. Optical Fault Induction Attacks // Cryptographic Hardware and Embeded Systems 2002. – Springer Lecture Notes in Computer Science, to appear. http://www.cl.cam.ac.uk/users/rja14/faultpap3.pdf.
4. Quisquarter J.J., Samyde D. Eddy Current for Magnetic Analysis with Active Sensor // Proc. of ESmart, 2002. - P.185-194.
5. Система численного физико-топологического двумерного моделирования полупроводниковых структур "DIODE-2"/ Ю.И.Сыцько, П.К.Скоробогатов, А.И.Чумаков и др. // Радиационная стойкость электронных систем - Стойкость-99": Тез. докл. Росс. научн. конф., г.Лыткарино, 1-3 июня 1999 г. - М.: СПЭЛС-НИИП, 1999. - С.21-22.