К. т. н. В. П. СИДОРЕНКО, В. Н. СИДОРЧУК, О. Н. ЗАБРОДИНА, к. т. н. Ю. Е. НИКОЛАЕНКО

Украина, г. Киев, НИИ микроприборов

Дата поступления в редакцию
15.03 2002 г.

Оппонент *к. т. н. Я. В. МАРТЫНЮК*
(НТУУ "КПИ", г. Киев)

ЭНЕРГОНЕЗАВИСИМАЯ ПАМЯТЬ НА ЭЛЕМЕНТАХ FLOTOX ДЛЯ БИС ЭЛЕКТРОННЫХ КАРТ

Рассмотрены вопросы построения электронных пластиковых карт многоразового использования с учетом ужесточения требований к их эксплуатационным параметрам.

В 1983 г. в пластиковую карту был внедрен микропроцессор — так родилась карта «с интеллектом». «Интеллектуальная» карточка позволяет: получить доступ к телефону-автомату; вести персональные записи, обеспечивая защиту доступа к данным; производить дистанционные финансово-расчетные операции в банках; служить стандартной кредитной карточкой или применяться в системах безналичного расчета для магазинов розничной торговли.

Под термином «интеллектуальная карточка» (smart card) в зарубежной литературе понимаются два вида разноцелевых устройств:

— запоминающее устройство или микроконтроллер для широкого спектра применений (карты памяти);

— кредитно-расчетная карточка индивидуального пользования со встроенными средствами обработки информации (интеллектуальные карты).

Карты памяти имеют встроенную микросхему. Все «интеллектуальные» возможности карт поддерживаются считывающим устройством, которое может читать и записывать в память карты. Существуют карты с различной емкостью памяти, реализуемой либо в виде программируемого постоянного запоминающего устройства — ППЗУ (которое позволяет считывать много раз, но в каждый адрес информация может быть записана только один раз), либо в виде электрически стираемого репрограммируемого ПЗУ (ЭС РПЗУ), которое позволяет перезаписывать и считывать многократно. Наибольшее распространение электронные карты памяти получили в области предоставления услуг телефонной связи с помощью таксофонов.

Смарт-карты внешне не отличаются от карт памяти, однако содержат «логику», что делает их «интеллектуальными». Микросхемы смарт-карт представляют собой полные микроконтроллеры (микропроцессоры) и содержат следующие компоненты:

— центральный процессор для обработки инструкций карты;

— оперативное запоминающее устройство (ОЗУ) для временного хранения данных, например, результатов вычислений, произведенных процессором;

— постоянное запоминающее устройство для хранения инструкций, используемых процессором, данных о владельце карты и т. п.;

— электрически стираемое репрограммируемое запоминающее устройство для хранения данных, изменяющихся в процессе эксплуатации карты (при этом содержимое памяти не должно теряться при отключении питания);

— систему ввода-вывода для обмена данными с внешними устройствами;

— встроенную операционную систему;

— встроенную систему безопасности для защиты данных с возможностью шифрования.

Смарт-карта по сути представляет собой небольшой компьютер, способный выполнять расчеты подобно персональному компьютеру. (Наиболее мощные современные смарт-карты сопоставимы с персональными компьютерами начала 1980-х годов.) В этих картах ЭС РПЗУ используется для хранения данных пользователя, которые могут считываться, записываться и модифицироваться. Смарт-карты имеют различную емкость памяти и обычно используются в приложениях, требующих высокой степени защиты (например, в финансовой практике).

Доступная для разработчиков БИС Украины производственная база позволяет успешно производить более простые по составу ИС *карты памяти*. Киевский НИИ микроприборов имеет опыт разработки интегральных микросхем для электронных карт памяти, применяемых в системах безналичных расчетов. Этот опыт показал, что создание всей системы безналичных платежей и успешное ее внедрение может быть осуществлено только при комплексном подходе — создании электронных карт, необходимого оборудования и программного обеспечения для оснащения всех участников системы.

В НИИ выполнены разработки специализированных интегральных схем для телефонной карточки одноразового и многоразового использования, ИС для предоплаты за пользование энергоносителями и БИС карты для безналичных расчетов в торговле и сфере услуг. Использование микросхемы в качестве носителя информации для электронных карт памяти потребовало введения многоступенчатой системы защиты данных от несанкционированного доступа, которая оказалась достаточно эффективной (с учетом затрат на защиту информации от мошенничества).

Комплекс специальных мер, включающих в себя возможность производства карточек только промыш-

ленным путем, занесение специальной информации производителем на этапе контроля микросхем и эмитентом карточек при ее электрической персонализации, возможность зачисления денег в карточку только после правильной подачи индивидуального секретного ключа, содержащегося в микросхеме, исключают возможность подделок и копирования карт, а также несанкционированный доступ.

Основные свойства защиты накопителя основаны на разделении памяти на различные функциональные области:

— область изготовителя для неизменных данных изготовителя кристалла;

— область персонализации для постоянных данных, относящихся к данным по применению;

— область применения для переменных данных, относящихся к данным по применению;

— защищенная область для несчитываемых данных.

Вышеуказанному делению областей памяти по их назначению соответствует деление энергонезависимой памяти на функциональные зоны — такие как ПЗУ, РПЗУ или чистое ЭС РПЗУ — в соответствии со специальной аппаратной логикой. Доступ по чтению к прикладным областям осуществляется после предъявления секретного кода. Каждая зона доступна для обновления только после предъявления специального кода, индивидуального для каждой зоны. Таким образом, одна зона может использоваться для записи максимальной суммы, разрешенной к расходованию, а вторая накапливает текущий расход. (Необходимо отметить, что разделение памяти на области напрямую связано с отработанной за рубежом в течение нескольких лет организацией и технологией проведения безналичных платежей за товары и услуги.)

Разработанные интегральные схемы карт памяти представляют собой ЭС РПЗУ для хранения данных, многократно изменяющихся в процессе эксплуатации карты; при этом содержимое памяти сохраняется при отключении питания. Ввод и вывод информации осуществляется в последовательном коде. Область памяти выполнена в виде матрицы X слов × 8 (или 16) ячеек и обладает идентификационными (ПЗУ) и персонализационными (РПЗУ) областями информации. Чтение и программирование осуществляются побитно, а стирание — побайтно.

Существует несколько вариантов реализации РПЗУ с электрическим стиранием информации. В них используются отличающиеся по размерам и конструкции запоминающие элементы с разными физическими процессами при записи и стирании информации, которые обладают также разными показателями долговечности (количество циклов перезаписи) и времени хранения информации. В качестве базовой ячейки памяти нами принят элемент FLOTOX, который обладает рядом эксплуатационных характеристик, превосходящих характеристики ЭС РПЗУ с другими типами ячеек (ЭС РПЗУ с УФ-стиранием информации, «быстрых» ЭС РПЗУ на FLASH-элементах памяти или МНОП-элементах памяти на «горячих» носителях и др.). К таким характеристикам относятся:

— возможность стирания информации отдельными байтами или даже битами;

— возможность реализации режимов стирания и записи во всем рабочем диапазоне температур от –60°С до +125°С за счет температурно-независимого механизма записи-стирания (туннелирования Фаулера—Нордхейма);

— низкоэнергетический характер переноса заряда при программировании, что позволяет реализовать схему с одним внешним источником питания для всех режимов работы (напряжение программирования ячейки памяти амплитудой 16—20 В формируется на кристалле) и временем программирования 5 мс;

— количество циклов перепрограммирования до 10^6;

— время непрерывного считывания информации не менее 5000 ч, а энергонезависимого хранения — не менее 10 лет (при считывании и хранении записанная информация не разрушается, т. е. в нормальных условиях работы ее регенерация не требуется);

— технологическая совместимость с базовыми технологическими маршрутами КМОП-технологии с поликремниевым затвором;

— простота реализации аппаратной и программной защиты хранимой информации от несанкционированного доступа.

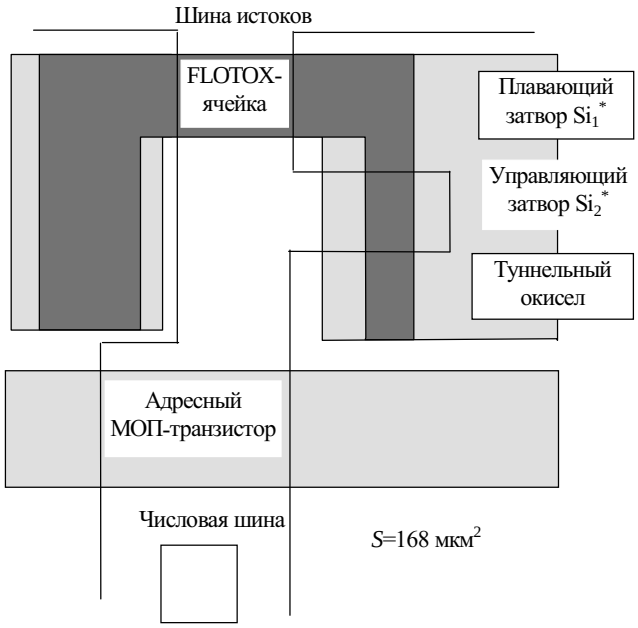

Рис. 1. Топология FLOTOX-элемента памяти

Для построения матрицы памяти на FLOTOX-приборах каждый запоминающий элемент выполняется на двух транзисторах (**рис. 1**): FLOTOX-прибор является собственно запоминающим элементом, а второй транзистор — транзистором выборки. Использование двух транзисторов является недостатком данного элемента памяти, т. к. не позволяет создать на его основе высокоплотный накопитель РПЗУ, который определяет размер кристалла и, в конечном счете, его стоимость.

В элементе FLOTOX область туннелирования, расположенная над стоком, используется как для заряда, так и для разряда плавающего затвора (первый уровень поликремния, на котором хранится информация).

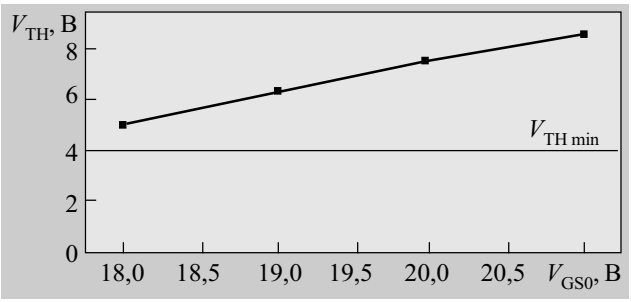

Рис. 2. Зависимость эффективности стирания от амплитуды импульса стирания V_{GS0} (длительность импульса стирания T_{ER}=5 мс)

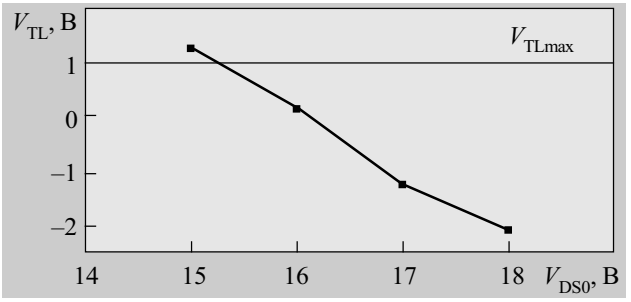

Рис. 3. Зависимость эффективности записи от амплитуды импульса записи V_{DS0} (длительность импульса записи T_{WR}=5 мс)

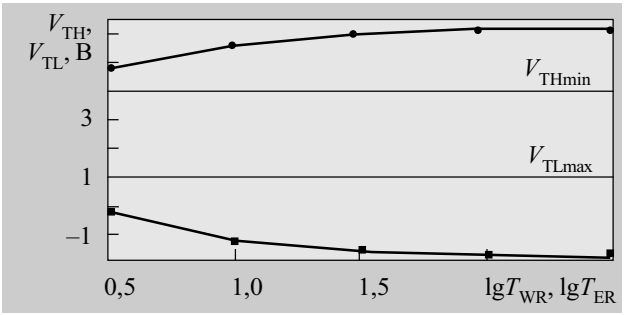

Рис. 4. Влияние длительности импульсов стирания T_{ER} (мс) и записи T_{WR} (мс) на эффективность программирования (амплитуда импульсов стирания V_{GS0} — 20 В, импульсов записи V_{DS0} — 18 В)

Работа FLOTOX-ячейки в режимах записи и стирания достаточно подробно описана в работах [1—4].

Логическая информация в накопителе ЭС РПЗУ отображается электрически изменяемым пороговым напряжением FLOTOX-ячейки. В режиме стирания элемент памяти переводится в состояние с высоким пороговым напряжением (V_{TH}>7 В), а в режиме записи — в состояние с низким пороговым напряжением (V_{TL}<–1 В). Величина порогового напряжения запоминающего транзистора и время стирания/записи информации зависят от напряжения на затворе, диэлектрической проницаемости слоев диэлектрика затвора, а также их толщины.

На **рис. 2—4** приведены вольт-амперные характеристики FLOTOX-ячейки после стирания и записи бита информации. Очевидно, что высокие напряжения программирования и большие длительности импульсов при записи/стирании крайне неудобны для потребителей БИС, т. к. увеличивают габариты аппаратуры, усложняют требования к источникам питания, удлиняют время перепрограммирования. (Время перезаписи информации в накопителе может составлять от десятков микросекунд до десятков миллисекунд.) С целью сокращения общего времени программирования в БИС предпочтительно использовать адаптивный алгоритм, который строится таким образом, что после программирования коротким (десятки микросекунд) импульсом встроенная в БИС схема производит контроль правильности записанной информации. Если результат контроля удовлетворителен, режим программирования завершается. В результате может быть достигнуто значительное сокращение времени программирования, что очень важно при пользовании карточкой.

По нашему мнению, сейчас в Украине выпуск электронных карт является достаточно дорогим производством, поэтому наиболее оптимальной и экономически целесообразной является реализация карточки многоразового использования, которая обеспечивает повторную перезагрузку при зачислении денег на нее. Однако в этом случае необходимо ужесточение требований к таким эксплуатационным параметрам FLOTOX-ячейки как циклоустойчивость и время хранения информации.

Цикл перепрограммирования включает стирание информации в ячейке и следующую за ним запись. При увеличении количества циклов перепрограммирования ($N_ц$) происходят необратимые изменения (деградация) электрических свойств туннельного окисла, связанные с захватом положительных и отрицательных зарядов и генерацией новых ловушечных состояний. Это приводит к ухудшению характеристик элементов памяти, использующих этот окисел.

Исследования показали, что при малых интегральных потоках электронов (<10^{16} эл/см^2) происходит захват положительного заряда вблизи N^+-монокремниевого электрода, а при больших потоках начинает преобладать захват электронов на исходные и вновь генерируемые ловушки, причем по всему объему окисла. Одновременно с этим происходит генерация ловушек положительного заряда, концентрация которых растет с увеличением интегрального потока инжектируемого заряда. После прекращения высокополевого воздействия происходит выброс положительного заряда с этих ловушек. Захват заряда на вновь генерируемые ловушки увеличивает проводимость туннельного окисла при пониженных полях и уменьшает — при высоких электрических полях. При увеличении количества циклов перепрограммирования (или интегрального потока заряда, прошедшего через туннельный окисел) пороговое напряжение ячейки памяти после стирания уменьшается. Причем темп уменьшения его тем выше, чем больше сечение захвата электронов, выше концентрация исходных ловушек в окисле и выше скорость генерации новых ловушек в окисле. При увеличении тока туннелирования возрастает темп захвата электронов на исходные ловушки и скорость генерации новых ловушек, что приводит к интенсивному ухудшению эффективности стирания.

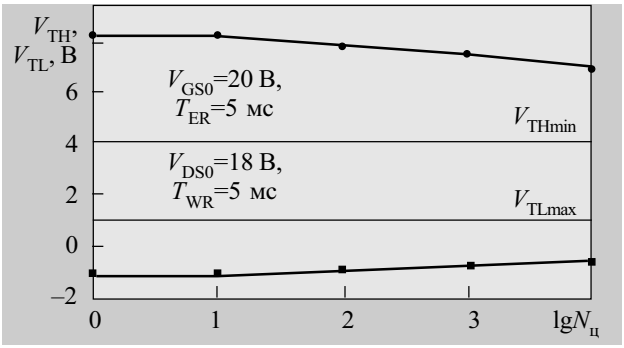

Рис. 5. Устойчивость ячейки памяти к циклам перепрограммирования

Полученные экспериментальные данные (**рис. 5**) показывают, что вплоть до 10000 циклов перепрограммирования не происходит существенной деградации параметров FLOTOX-ячейки, что вполне удовлетворяет требованиям к БИС электронных карт памяти.

Другим важнейшим для потребителя параметром является время хранения данных. Различают два режима: хранение в «активном» режиме и энергонезависимое хранение. Активным принято считать режим, когда на ИС подано напряжение питания, а к ячейке, находящейся в режиме хранения данных, есть обращение либо нет обращения. Энергонезависимым принято считать хранение информации, когда на схему не подано напряжение питания.

В *активном* режиме при хранении положительного заряда главную роль играет ток утечки через туннельный окисел. В результате воздействия инжектированного тока туннелирования, как отмечалось выше, происходит захват положительных зарядов вблизи N^+-электрода, отрицательного заряда по всему объему окисла и генерация мелких ловушек около зоны проводимости окисла. Глубина залегания ловушки отсчитывается от дна зоны проводимости для электронов и потолка валентной зоны для дырок. Мелкие ловушки (E ловушки намного меньше E_g, где E_g — ширина запрещенной зоны [5, с. 148]) повышают проводимость пленки окисла, а захваченный положительный заряд приводит к увеличению локального поля в окисле, примыкающем к стоку, что облегчает протекание тока Фаулера—Нордхейма от N^+-области стока к положительно заряженному плавающему затвору и приводит к потере информационного заряда. Ток надбарьерной эмиссии, ток смешанной термополевой эмиссии и дефекты в системе Si—SiO_2—Si* (Si* — поликремний) увеличивают потерю положительного информационного заряда. Наблюдается (**рис. 6**) сильная зависимость времени хранения положительного заряда от толщины туннельного окисла и приложенного напряжения считывания.

При активном хранении на плавающем затворе отрицательного заряда поле на туннельном окисле значительно слабее, чем в случае положительного заряда, а увеличенное поле на толстом межзатворном полиоксиде существенно меньше известных из литературы полей [6, 7], при которых в полиоксиде возникает заметная проводимость, приводящая к стеканию отрицательного заряда на управляющий затвор. На практике она возникает только при очень сильной шероховатости поверхности поликремниевого затвора, на пиках зерен поликремния, т. е. в местах концентрации электрических полей [8].

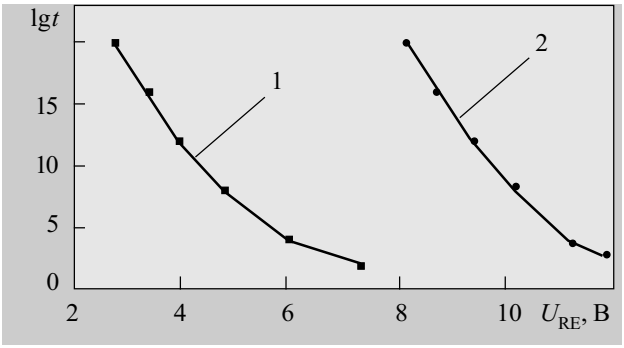

Рис. 6. Расчетная зависимость времени хранения информации после записи (t, с) от напряжения считывания (U_{RE}) и толщины туннельного окисла ($d_{тун}$):
1 — $d_{тун}$=8 нм; *2* — $d_{тун}$=13 нм

Более существенным, на наш взгляд, является стекание отрицательного заряда с плавающего затвора при хранении в *пассивном* режиме. В этом случае на ИС не подается напряжение питания, и все электроды ячейки, за исключением плавающего затвора, находятся под равным нулевым потенциалом. Скорость стекания заряда определяется величиной и местоположением в окисле захваченных положительных и отрицательных зарядов. Для наших условий захвата и из-за наличия зоны обеднения в монокремнии положительный заряд и в пассивном режиме будет стекать быстрее.

В реальной ситуации сужение межпороговой зоны элемента памяти происходит одновременно как во времени, так и при воздействии циклов перепрограммирования. Наихудшим случаем является воздействие максимально допустимого числа циклов перепрограммирования в начальный период эксплуатации ИС и последующее хранение в течение гарантируемого интервала времени. В процессе эксплуатации ИС деградация элементов памяти в пределах накопителя носит случайный характер и зависит от интенсивности обращения к каждой конкретной ячейке со стороны потребителя.

Особенности конструкции и функционирования, параметрические зависимости FLOTOX-ячеек памяти должны быть тщательно учтены при согласовании накопителя со схемами обрамления БИС (особенно в режимах считывания и программирования). При правильном проектировании БИС с FLOTOX-ячейкой памяти потребитель получит электронную карту с высокими техническими характеристиками, работающую в широком температурном диапазоне с одним источником питания во всех режимах. К преимуществам следует также отнести технологическую совместимость FLOTOX-ячейки с базовой КМОП-технологией, что позволяет существенно снизить цену кристалла БИС.

Ведущие производители БИС для электронных карт, используя новейшие достижения в области технологии, непрерывно совершенствуют FLOTOX-элемент памяти, поскольку он, в конечном счете, определяет характеристики и цену изделия в целом. Разработаны однотранзисторные FLOTOX-ячейки, использующие качественно новые пленки диэлектрика с улучшенными параметрами. Важным преимуществом такого запоминающего элемента являются ма-

лые геометрические размеры, позволяющие создать на его основе высокоплотный накопитель РПЗУ большой информационной емкости с отличными эксплуатационными параметрами — один источник питания 1,5—3 В во всех режимах, время программирования — десятки микросекунд, время хранения в активном режиме не менее 15000 часов и не менее 10^6 циклов перепрограммирования.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Сидоренко В. П., Забродина О. Н., Сидорчук В. Н., Николаенко Ю. Е. БИС электронных пластиковых карт с предварительной оплатой // Технология и конструирование в электронной аппаратуре.— 2001.— № 3.— С. 53 — 57.

2. Brattacharyya A. Effect of trapping in thin oxides on the writes and erase characteristics of floating gate EEPROM devices // Journal of Phisics D: Applied Phisics.— 1984.— Vol. 17, N 4.— P. 799 — 803.

3. Brattacharyya A. Modeling of writes/erase and charge retention characteristics of floating gate EEPROM devices // Solid-State Electronics.— 1984.— Vol. 27, N 10.— P. 899 — 906.

4. Tanaka S., Ishicawa M. One-demention writing model of N-chennel floating gate ionization MOS (FIMOS) // IEEE Transactions on Electron Devices.— 1981.— Vol. ED-28, N 10.— P. 1190 — 1197.

5. Бонч-Бруевич В. Л., Калашников С. Г. Физика полупроводников.— М.: Наука, 1990.

6. Anderson P. M., Kerr D. R. Evidence for surface asperity mechanism of conductivity in oxide grown on polycristalline silicon // Journal of Applied Phisics.— 1977.— Vol. 48, N 11.— P. 4834 — 4836.

7. Heimann P. A., Murarca S. P., Sheng T. T. Electrical conduction and breakdown in oxides of polycristalline silicon and their correlation with interface texture // Journal of Applied Phisics.— 1982.— Vol. 53, N 9.— P. 6240 — 6245.

8. Корнющкин Н. А., Ковчавцев А. П., Сапожникова А. Н., Французов А. А. Токи утечки через окисел, выращенный на поверхности затвора из поликристаллического кремния // Микроэлектроника.— 1983.— Т. 12, вып. 3.— С. 210 — 216.