нималось только путем голосования участников Третьей Конференции (апрель 2000г.). Именно по результатам этого голосования (RIJNDAEL-86, SERPENT 59, TWOFISH-31, RC6-23, MARS-13) в качестве стандарта XXI века был рекомендован алгоритм RIJNDAEL, полученный в ходе реализации проекта AES.

Исследования, проведенные авторами, показали, что отмеченная проблема может быть решена с позиций подхода, предполагающего виртуальные представления процесса шифрования. Применение данного подхода позволило получить аналитические выражения для эффективности $D(\Phi,u)$ шифрования и создать программный комплекс оценки качества защиты информации (рис.1), к основным отличительным особенностям которого следует отнести: 1) возможность количественной оценки эффективности шифрования, в том числе в реальном масштабе времени; 2) учет статистических характеристик ансамблей сообщений, ключей и криптограмм, участвующих в процессе шифрования; 3) учет влияний информационных характеристик (в первую очередь избыточности) источников сообщений.

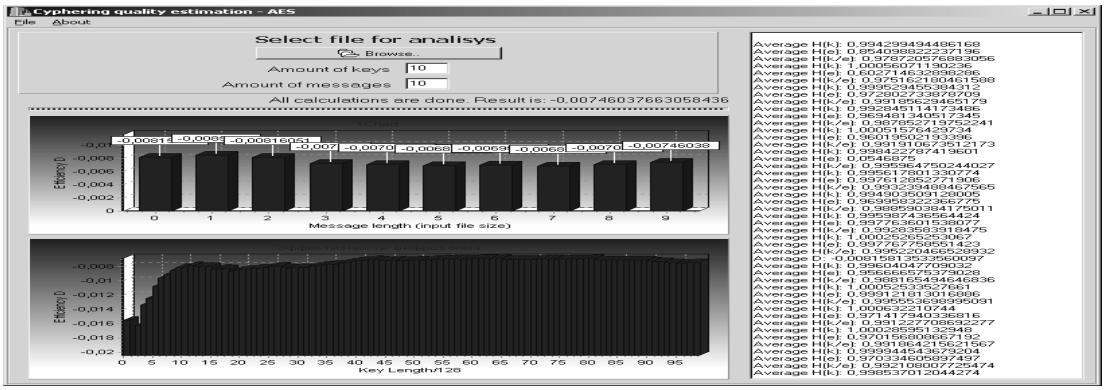

Рисунок 1

Применение созданного комплекса для оценки качества перечисленных выше шифров подсказало правомочность рекомендаций NIST. Так, эффективность алгоритма RIJNDAEL (рис. 1) составило для источников u_A английского языка:

$$D(\Phi,u_A) = -7.4604*10^{-3},$$

что соответствует более высокому качеству защиты по сравнению с алгоритмом SERPENT, у которого

$$D(\Phi,u_A) = -8.0781*10^{-3}.$$

Отрицательные значения $D(\Phi,u_A)$ означают, что эти алгоритмы не обеспечивают условия теоретической недешифруемости, которые восполняются при $D(\Phi,u\ ) \geq 0$. В данном случае более высокое качество шифрования характеризует приближенные значения $D(\Phi,u\ )$ к нулю в отрицательной области.

Применение предложенного подхода и созданного на его основе программного комплекса открывает принципиально новую область исследований в направлении оценки качества защиты информационных технологий. Приведенные результаты получены при поддержке гранта Министерства Образования РФ Т02-03.1-816.

ЭЛЕКТРОННОЕ УПРАВЛЕНИЕ ПЕРЕХОДОМ МЕТАЛЛ-ИЗОЛЯТОР В ДВУОКИСИ ВАНАДИЯ

Кулдин Н.А., Величко А.А., Стефанович Г.Б.,
Пергамент А.Л., Стефанович Д.Г.
Петрозаводский государственный университет, Петрозаводск

Переход металл-изолятор в оксидах переходных металлов перспективен для создания электронных устройств, реализующих в той или иной форме резкое пороговое изменение электрических и оптических свойств при достижении внешними параметрами определенного критического значения. Несмотря на универсализм поведения, системы с ПМИ условно могут быть разделены на две группы по начальному механизму нестабильности основного состояния [1]. В первой группе изменения в кристаллической решетке (структурный фазовый переход) приводят к расщеплению электронной зоны проводимости и, следовательно, к переходу в изоляторное состояние. В другой группе ПМИ удовлетворительно описывается в рамках чисто электронных моделей (переход Мотта).

Классическим объектом для изучения ПМИ является диоксид ванадия, в котором наблюдается фазовый переход 1 рода при достижении критической температуры перехода T_t=68^{o}C [1]. В ряде работ изучалось влияние электрического поля на ПМИ в планарных структурах на основе VO_2 [2,3], и было обнаружено влияние электрического поля на характеристики переключения или перехода, однако обнаруженные эффекты были слабыми и не поддавались однозначной интерпретации. В частности, влияние поля на температурную зависимость проводимости диоксида ванадия может быть объяснено сквозными

токами утечки через подзатворный диэлектрик вызывающими дополнительный джоулев разогрев пленки VO_2.

По нашему мнению, тепловое влияние может быть исключено при исследовании эффекта поля в структурах типа $Si\text{-}SiO_2\text{-}Si_3N_4\text{-}VO_2$. Следует отметить, что эксперименты в подобных структурах в условиях статического эффекта поля могут оказаться малоэффективными, так как для создания поверхностного потенциала, обеспечивающего значительное увеличение концентрации в слое достаточной глубины, требуется, видимо, приложить напряжение затвора V_G сравнимое с напряжением пробоя диэлектрика. Более перспективным может оказаться подход, основанный не на эффекте поля, а на инжекции носителей заряда извне. Реализуя инжекцию носителей через слой окисла в нитрид кремния, можно обеспечить в нем накопление большого по величине заряда. В том случае, когда слой нитрида достаточно тонкий, захваченный заряд будет создавать электрическое поле на внешней стороне структуры, а оно в свою очередь будет воздействовать на электронную подсистему VO_2.

В эксперименте использовались структуры двух типов, в которых в качестве подложки был выбран кремний n-типа с толщиной оксида 60 нм, а нитрида 100 нм (I тип), и кремний p-типа, с толщиной оксида 50 нм и нитрида 100 нм (II тип). Диоксид ванадия наносился на поверхность полупроводниковой структуры методом магнетронного реактивного распыления с последующим нанесением алюминиевых электродов. После изготовления тестовых структур измерялись вольт-фарадные характеристики и скачок проводимости при ПМИ в диоксиде ванадия. Затем осуществлялась туннельная инжекция электронов (в структурах I типа) и дырок (в структурах II типа) и их накопление в нитриде. Для реализации туннельной инжекции электронов или дырок, на металлический электрод, нанесенный на подложку, давалось импульсное напряжение ($V \le 110$ В, $t = 0{,}1$ мкс, $f = 10^3$Гц).

Накопление заряда контролировалось измерением вольт-фарадных характеристик по сдвигу напряжения плоских зон (ΔV_{FB}). ΔV_{FB} зависело от типа подложки, величины импульса инжекции и времени инжекции и достигало значений $\Delta V_{FB} \approx 6 - 12$ В. После этого четырехзондовым методом измерялась проводимость диоксида ванадия. Влияния электрического поля накопленного в нитриде заряда для структур I типа обнаружено не было, тогда, как для структур II типа наблюдалось смещение температурной зависимости проводимости (гистерезисная кривая) в область низких температур (рис.1).

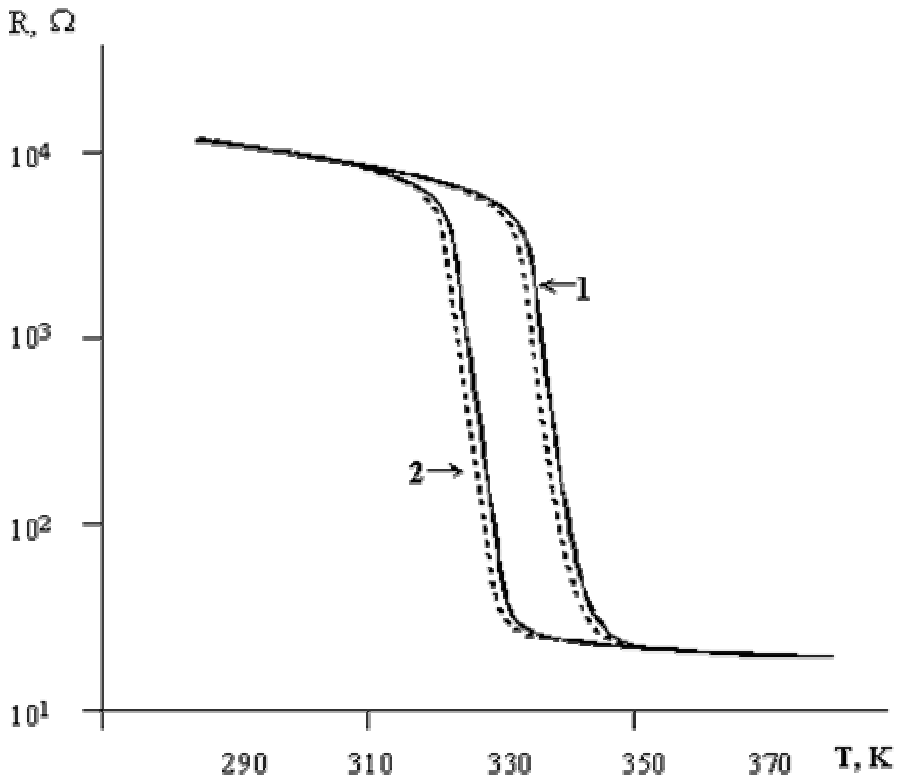

Рисунок 1. Зависимость сопротивления (R) VO_2 от температуры (T): 1 – в исходном состоянии; 2 – после накопления заряда.

Смещение температурной зависимости проводимости для структур II типа, по нашему мнению, обусловлено увеличением концентрации электронов в слое VO_2 на границе с нитридом кремния, что приводит к снижению температуры перехода в этой области (переход Мотта).

Полученные результаты подтверждают влияние эффекта поля на ПМИ в условиях исключающих тепловое действие токов утечки через изолятор, что позволяет рассматривать пленочные структуры на основе диоксида ванадия потенциальными базовыми

элементами для быстродействующих устройств микро- и оптоэлектроники.

Работа выполнена при поддержке гранта Министерства Образования РФ и Американского Фонда Гражданских Исследований и Развития (CRDF) № PZ-013-02.

Список литературы:

1. Бугаев А.А., Захарченя Б.П., Чудновский Ф.А. // Фазовый переход металл-полупроводник и его применение. Л.: Наука, 1979. - 183 с.

2. Мокроусов В.В., Корнетов В.Н., // ФТТ. 1974. Т.16. В.10. С. 3106 – 3107

3. Васильев Г.П., Сербинов И.А., Рябова Л.А. // Письма в ЖТФ. 1977. Т.3. В.8.

АЛГОРИТМ ПОИСКА ИНФОРМАЦИИ В РЕЛЯЦИОННЫХ БАЗАХ ДАННЫХ, НОРМАЛИЗОВАННЫХ НА ОСНОВЕ ОПЕРАЦИЙ ВЫБОРКИ И СОЕДИНЕНИЯ

Лидовской К.В., Маликов А.В.
Северо-Кавказский государственный технический университет, Ставрополь

Рассматриваются реляционные базы данных (РБД) нормализованные на основе операций выборки и соединения [1], структура которых представлена на рисунке 1.

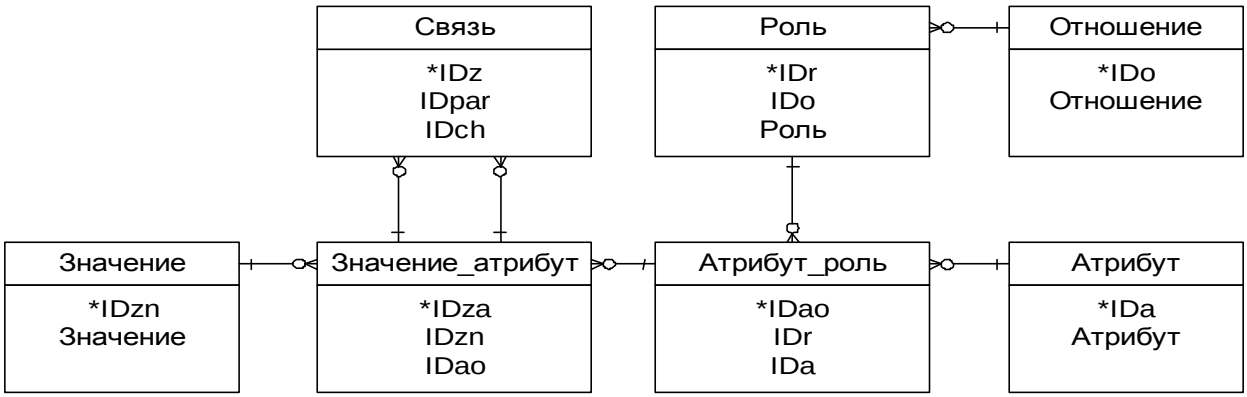

Рисунок 1. Структура реляционных баз данных, нормализованных на основе операций выборки и соединения

Представленной структурой может быть описана любая предметная область, т.к. для всякого атомарного значения отношения можно построить ориентированный граф связей с другими значениями. В качестве примера в представленной структуре реализована следующая информационная модель (рисунок 2).

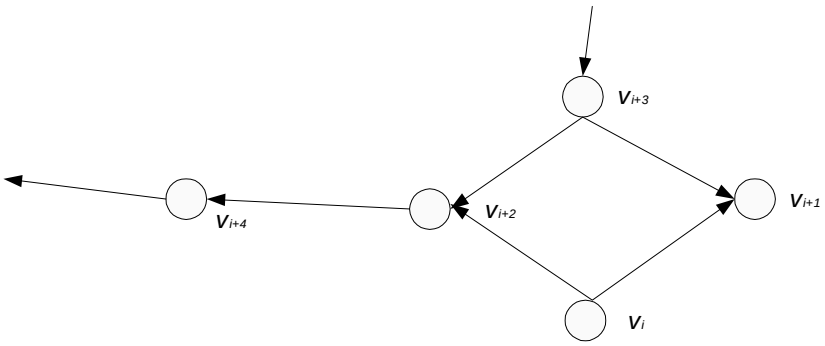

Рисунок 2. Ориентированный граф связей некоторого подмножества атомарных значений реляционной базы данных

Перерисуем граф связей подмножества значений РБД, в виде ориентированной сети (рисунок 3).

Для разработки декларативного языка запросов к РБД со структурой, представленной на рисунке 1, необходимо определить алгоритм поиска информации на ориентированной сети. Как правило, пользовательские запросы формируются на выборку фиксированного набора атомарных значений по другим известным значениям.

Между любыми двумя значениями, если существует связующий их путь, то он однозначен. Точнее определить его как поисковый путь, чтобы отличать его от пути графа. Движение по связям разрешено в обе стороны: по направлению стрелки переход будем называть уточняющим, против стрелки — обобщающим.