СЕКЦИЯ 3. ТЕХНИЧЕСКИЕ СРЕДСТВА ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

ДАТЧИК ОБНАРУЖЕНИЯ УТЕЧЕК ИНФОРМАЦИИ В КАНАЛЕ ОТКРЫТОЙ ЛАЗЕРНОЙ СИСТЕМЫ СВЯЗИ

К.В. МЕЛЬНИКОВ

Разработан датчик (широкополосное фотоприемное устройство с высокой чувствительностью) с параметрами, позволяющими использовать его в качестве устройства, обнаруживающего утечку информации в открытых каналах оптической связи.

Фотоприемник обладает чувствительностью порядка 20 нВт и полосой пропускания 25 МГц (35 Мбит/с) и может работать с оптическими излучениями в диапазоне длин волн 850–1570 нм.

В качестве оптоэлектрического преобразователя использован арсенидогаллиевый лавинный фотодиод фирмы *EG&G* типа C30662E с диаметром фоточувствительной площадки 200 мкм. Для повышения стабильности характеристик применена температурная стабилизация фотодиода на уровне +15˚C.

Устройство включает в себя входной каскад, каскад с регулируемым усилением (±40 dB), детектор уровня шумов, компаратор, выходной формирователь и схему термостабилизации.

Измерения проводились сравнительным методом. В качестве источника сигнала использовался лазерный диод фирмы *Siemens* SFH495P с рабочей длиной волны 980 нм. В качестве эталонных приемников использовались ФПУ-03Д НИИ *"Полюс"* (г. Москва) на основе германиевого ЛФД и Model 757-02 фирмы *Analog Modules* (США) на основе *InGaAs* PIN-фотодиода диаметром 300 мкм.

Результаты измерений показали уровень чувствительности разработанного устройства в диапазоне 20±5 нВт.

МИКРОВЗРЫВ В ПОРИСТОМ КРЕМНИИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПОПЫТКЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КРЕМНИЕВЫМ ЧИПАМ

А.В. ДОЛБИК, А.А. КОВАЛЕВСКИЙ, В.А. ЛАБУНОВ, С.К. ЛАЗАРУК, Д.Н. УНУЧЕК

С тех пор как появились первые чипы микросхем — появились и люди, взламывающие эти чипы. И точку в соревновании защиты и нападения, по-видимому, поставят не скоро. Учитывая, что подложка большинства микросхем кремниевая, то можно изготовить кремниевые чипы, которые бы саморазрушались при попытке их несанкционированного вскрытия. Недавно обнаруженная взрывная реакция в пленках наноразмерного пористого кремния может быть использована для этого случая, что обеспечит защиту информации, хранимой на чипе [1].

Явление взрыва пористого кремния инициируется механическим, электрическим либо химическим способом [2]. Микровзрыв, наблюдаемый при реакции окисления пористого кремния, обусловливается целым рядом химических реакций.

В связи с этим проведен анализ реакций имеющих место при окислении путём расчёта изобарно-изотермического потенциала ΔG. ΔG является оценочной величиной для расчёта количества теплоты, выделяемой в ходе реакции. Из проведённого расчёта определено, что такими реакциями являются реакции с участием групп силана *SiH*, SiH_2, SiH_3, водорода, кислорода. Также важны разрывы *Si-Si* связей. Хотя не исключены и другие реакции, характеризующиеся отрицательной величиной ΔG.

На основании проведенного анализа разработан технологический маршрут изготовления саморазрушающихся кремниевых чипов, обратная сторона которых покрыта слоем пористого кремния. Показано, что разрушение кремниевого чипа можно вызвать электрической искрой, локальным нагревом либо механическим воздействием.

Управляемый микровзрыв пористого кремния позволяет разработать микросистемы, обладающие принципиально новыми возможностями в плане защиты информации.

Литература

1. D. Kovalev, V.Y. Timoshenko, N. Kunzner, E. Gross,F. Koch, Phys. Rev. Lett. 2001, Vol. 87, p. 68301.
2. F.V. Mikules, J.D. Kirtland, M.J. Sailor, Adv.Mater. 2002, Vol. 14,p. 38.

ОПТИЧЕСКИЕ МЕЖСОЕДИНЕНИЯ КРЕМНИЕВЫХ ЧИПОВ, КАК СПОСОБ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

А.В. ДОЛБИК, В.А. ЛАБУНОВ, С.К. ЛАЗАРУК, Е.Л. ПЕТРОВИЧ, Д.Н. УНУЧЕК

Привычные в прошлом металлические линии связи все чаще обнаруживают свои недостатки в новом столетии. Современные технологии уже исчерпали их возможности в быстродействии, и, кроме

того, электрические соединения являются потенциальными источниками утечки информации. Оптические линии связи обладают рядом преимуществ, из которых особо выделим высокую степень защиты информации, так как оптическая развязка компьютерных чипов надежно предотвращает потери информации, что наряду с высокой помехоустойчивостью, информационной емкостью и возможностью работы с высокой тактовой частотой дает оптическим линиям связи преимущества перед электрическими.

Давняя проблема оптического передатчика, похоже, найдет свое решение в активно исследуемом направлении пористого наноструктурированного кремния. На сегодняшний день для светодиодов на пористом кремнии нами получены следующие параметры: пороговые напряжение и плотность тока при светоизлучении составляют 4 В и 0,02 мА/см² соответственно. Время нарастания светового импульса 2 нс. Частота 200 Мгц. Единственный параметр, не удовлетворяющий требованиям для оптических межсоединений — квантовая эффективность светоизлучения. При необходимых 10 %, получена величина около 1 %. Изготовлен прототип кремниевых оптических межсоединений, демонстрирующий возможность использования фотонов при передаче и приеме информации как внутри кремниевого чипа, так и между соседними кремниевыми кристаллами.

Показаны перспективы использования оптических межсоединений для совершенствования технологий по обработке и защите информации.

ОСОБЕННОСТИ ВЫБОРА СРЕДСТВ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ ИЗ КОМПЬЮТЕРОВ ПО СЕТИ ЭЛЕКТРОПИТАНИЯ

И.М. РУСАК, В.П. ЛУГОВСКИЙ.

Общеизвестно, что работа о защите информации является жизненно необходимостью, поскольку в современных условиях выигрывает тот, кто владеет информацией. В проблеме утечек информации пока еще недостаточно внимания уделялось внешне малоприметному каналу передачи данных через сеть электропитания. Сигналы, попавшие в сеть, могут распространяться на большие расстояния и, учитывая разветвленную структуру сетевых проводников, представляющих в целом двухпроводные, линии связи, могут быть доступны нежелательным пользователям. Спектр наводимых сигналов простирается вплоть до диапазона десятков и сотен мегагерц.

Одним из основных путей предотвращения утечек данных по сети электропитания является применение фильтров. Фильтры для подавления сигналов проводимости разрабатываются из учета работы в диапазоне от 0,15 до 300 МГц. Основным требованием является высокая эффективность работы фильтров в диапазоне от 0,15 до 20 МГц, из-за высоких уровней помех от импульсных блоков питания.

Исходя из этих требований, основное подавление утечек данных производится с помощью дросселей в проводах питания, включенных как синфазно, так и противофазно. Для работы высокочастотной области диапазона (от 10 до 300 МГц) применяют проходные емкости, устанавливаемые на входе и выходе фильтра. Сама конструкция фильтра должна исключать возможность наводки электромагнитного излучения на элементы фильтра. Установку фильтра в устройство рекомендуется осуществлять внутри общего экрана корпуса ПЭВМ. Подобный фильтр применяется, в основном, для подавления кондуктивных сигналов от импульсного блока питания. Для подавления сигналов от модулей ПЭВМ установку фильтров необходимо осуществлять непосредственно около разъемов питания модулей. Роль модулей, как генераторов сигналов с наиболее широкой полосой, накладывает определенные требования на фильтры, устанавливаемые на модулях устройства. Эти фильтры должны подавлять помехи в очень широкой полосе частот (от 10 до 300 МГц). Нижняя граница частоты среза для фильтров определяется конструкцией ПЭВМ, в частности, длиной кабелей питания и интерфейсов. Верхняя граница частоты среза определяется элементной базой, применяемой в ЭВМ. Основное требование-подавление помех в диапазоне от 60 до 300 МГц. Помехи с более низкой частотой могут подавляться фильтрами, установленными в блоках питания устройства.

Подобные фильтры должны быть выполнены с учетом требований на невосприимчивость к внешнему излучению": либо корпус фильтра должен экранировать фильтр, либо установка фильтра и его конструкция (конфигураций сердечника) должна исключать возможность наводки на него внешних помех. При применении фильтров необходимо учитывать падение напряжения на элементах фильтра (дросселей). Построенные таким образом фильтры подавляют сигналы по каналу проводимости и уменьшают вероятность возникновения наводок излучения от проводов питания, что является универсальным методом борьбы одновременно с двумя видами утечек данных.

ИНТЕЛЛЕКТУАЛЬНАЯ ТЕХНОЛОГИЯ И ОБОРУДОВАНИЕ ДЛЯ ЗАЩИТЫ ОТ ПОДДЕЛКИ МАТЕРИАЛЬНЫХ ОБЪЕКТОВ

В.М. КОЛЕШКО, Ю.Д. КАРЯКИН, В.Л. БУРШ

Технология, не имеющая аналогов в мировой практике, предназначена для защиты от подделки, подмены или фальсификации любых материальных объектов в различных областях деятельности человека. Технология и оборудование защищены патентами на изобретение.

Разработанное оборудование позволяет: