Атаки методом оптического наведения ошибок

С.П. Скоробогатов, Р.Дж. Андерсон
Кембриджский Университет, Компьютерная Лаборатория
{sps32, rja14}@cl.cam.ac.uk

Мы описываем новый класс атак на смарткарты и защищенные микроконтроллеры. Облучение отдельного транзистора заставляет его проводить ток, тем самым внося ошибку в работу устройства. Такие воздействия имеют большой практический интерес; они даже не требуют дорогостоящего лазерного оборудования. Мы провели их используя сэконд-хэнд фотовспышку купленную за $30 в фотомагазине и лазерную указку за $8. Как иллюстрацию мощности этих атак мы разработали технику установки и сброса любого отдельного бита статического ОЗУ в микроконтроллере. Если не принять соответствующих мер оптические атаки могут быть использованы для наведения ошибок в протоколах и алгоритмах шифрования, а также для изменения работы процессора. Таким образом эти атаки дают мощное дополнение к уже существующим техникам глитчинга (кратковременного сбоя) и анализа сбоев в работе. Чувствительность к нашим атакам может создать большие проблемы для индустрии, подобные микропробингу в середине 90-х и анализу потребляемой мощности в конце 90-х.

Поэтому мы разработали технологию для защиты от этих атак. Мы используем самотактируемую двухпроводную логику для дизайна схем, где логическая 1 или 0 закодированы не высоким или низким напряжением на одной линии, а (HL) или (LH) сочетанием на паре линий. Комбинация (HH) сигнализирует опасность, которая приведет к сбросу процессора. Схемы могут быть разработаны таким образом, что сбой в одном транзисторе не приведет к сбою в защите. Эта технология может также сделать анализ потребляемой мощности очень труднореализуемым.

1 Введение

Смарткарты и защищенные микроконтроллеры разработаны таким образом, что они должны сохранять как секретность, так и целостность важной информации. Недостаточно только защититься от того, чтобы взломщик нашел значение хранящегося ключа для шифрования, нужно также, чтобы он не смог установить часть ключа в требуемое значение или внести ошибки в процесс расчета и

восстановил важную информацию. Такими ошибками могут быть ошибки данных, такие как некорректная цифровая подпись, приводящая к утечке ключа для подписи [1], или ошибки в исполняемом коде, такие как пропущенный условный переход, который уменьшает число циклов в блочном шифровании [2]. До сих пор наиболее известной техникой наведения таких ошибок был глитчинг – внесение скачка напряжения в цепь питания или линию тактового сигнала атакуемого чипа. Однако большинство современных чипов разработаны таким образом, чтобы противостоять глитчингу.

Обзор защиты от проникновения в смарткартах и защищенных микроконтроллерах может быть найден в [3]. Атаки могут быть инвазивные, использующие оборудование для тестирования чипов, такое как станции микропробинга и станции с фокусированным пучком ионов (FIB), для непосредственного извлечения данных из чипа; или неинвазивные включающие анализ электромагнитного излучения от чипа, использование ошибок в дизайне протоколов и другие уязвимости, которые могут проявляться внешне. Любой вид атак может быть активным или пассивным. Стандартная пассивная инвазивная атака включает использование микропробников для наблюдения шины данных смарткарты при ее работе; при активной атаке сигналы могут быть также введены извне, классический пример – это подключение заземленной иглы микропробника на тактовый вход декодера команд процессора для блокировки команды перехода. Пример пассивной неинвазивной атаки – это анализ электромагнитного поля вблизи тестируемого устройства [4], тогда как глитчинг – это классический пример активной атаки.

До сих пор инвазивные атаки требовали достаточно большого капиталовложения в лабораторное оборудование плюс определенные усилия для каждого атакуемого чипа. Неинвазивные атаки, такие как анализ потребляемой мощности, требуют только умеренных капиталовложений и усилий для разработки метода воздействия на конкретный тип устройства, зато потом стоимость атаки на каждое новое устройство достаточно низкое. Таким образом, неинвазивные атаки значительно более привлекательны если их можно осуществить.

К сожалению для взломщиков, в настоящее время многие производители микрочипов встраивают защиту от наиболее очевидных неинвазивных атак. Эти защиты включают

рассинхронизацию по тактовой частоте, делающую труднее анализ потребляемой мощности, и схемы, которые реагируют на глитчинг, сбрасывая процессор. В то же самое время, инвазивные методы атак становятся сложнее и дороже, поскольку чипы становятся все сложнее и размеры транзисторов в них уменьшаются. Поэтомы мы разработали новые, более мощные методы атаки чипов.

Мы описываем наш новый класс атак как ‘полуинвазивные’. Под этим мы подразумеваем что, как инвазивные атаки, они требуют распаковки чипа для доступа к поверхности кристалла. Но слой пассивации на чипе остается нетронутым – полуинвазивные методы не требуют электрического контакта к металлическим линиям, т.о. сам кристалл не подвергается разрушению.

Полуинвазивные атаки не новы. Анализ электромагнитного излучения [4] лучше проводится на распакованном чипе, и старый трюк со стиранием бита защиты в микроконтроллере путем облучения его ультрафиолетовым светом тоже требует распаковки чипа. Теоретически полуинвазивные атаки могут быть проведены с использованием таких средств как ультрафиолетовое и рентгеновское излучение, лазеры, электромагнитные поля и локальный нагрев. Они могут быть использованы как в отдельности, так и в сочетании друг с другом. Однако эта область еще не была исследована.

Сейчас мы продемонстрируем как очень мощные атаки могут быть проведены быстро и используя дешевое и простое оборудование.

2 Предыстория

После открытия и внедрения полупроводникового транзистора было обнаружено, что он по сравнению с радиолампами гораздо более чувствителен к ионизирующему излучению вызываемому ядерным взрывом, радиоактивными изотопами, рентгеновским излучением или космическими лучами. В середине 60-х при экспериментах с импульсными лазерами было обнаружено, что когерентное излучение вызывает подобные явления. Лазеры начали использоваться для симулирования воздействия ионизирующего излучения на полупроводники [5].

С тех пор технология сделала огромный прорыв. Дорогие лазеры на инертных газах и твердотельные лазеры были заменены недорогими

полупроводниковыми лазерами. В результате технология переместилась из лаборатории в потребительскую электронику.

Лазерное излучение способно ионизировать полупроводниковые области интегральной схемы если энергия его фотонов превышает ширину запрещенной зоны полупроводника. Излучение с длиной волны 1.06мкм (энергия фотонов 1.17эВ) использованное в [6] имело глубину проникновения около 700мкм и давало равномерную пространственную ионизацию кремниевых устройств. Однако дисперсия ограничивает его фокусировку до нескольких микрон, что недостаточно для современных полупроводниковых устройств. Хотя при переходе от инфракрасного к видимому свету поглощение фотонов стремительно возрастает [7], использование красного и зеленого лазеров стало возможным поскольку транзисторы в современных чипах стали тоньше. Меньший размер устройств также означает, что для достижения того же уровня ионизации необходимо меньше энергии.

В случае с КМОП устройствами существует опасность защелкивания схемы, вызывающая короткое замыкание и приводящая к выходу устройства из строя. Поэтому использование радиации на КМОП структурах должно проводиться с соответствующими предосторожностями.

Хотя существует множество публикаций об использовании импульсных лазеров для симулирования ионизирующего излучения, мы не смогли найти никаких публикаций об использовании лазеров для контроля или изменения состояния интегральных схем. Поэтому мы решили попробовать воздействовать интенсивным источником света на полупроводниковый чип, и в особенности на КМОП логику, с тем, чтобы определить возможно ли изменить состояние ячейки памяти и если да, то насколько это трудно.

Наш первый эксперимент был проведен на статическом ОЗУ. Структура стандартной шеститранзисторной ячейки КМОП статического ОЗУ показана на Рис.1 [8].

Две пары p- и n-канальных транзисторов образуют триггер, в то время как два других n-канальных транзистора используются для чтения его состояния и записи в него новых значений. Топология ячейки показана на Рис.2 [9]. Транзисторы T_1 и T_3 образуют КМОП инвертор; вместе с другой подобной парой они образуют триггер, который контролируется транзисторами T_5 и T_6.

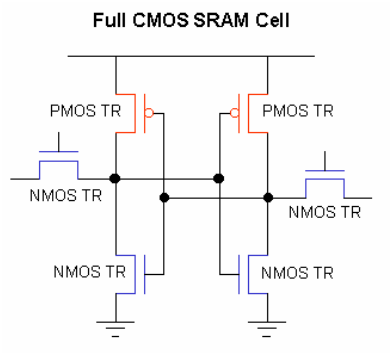

Рис.1. Структура ячейки статического ОЗУ

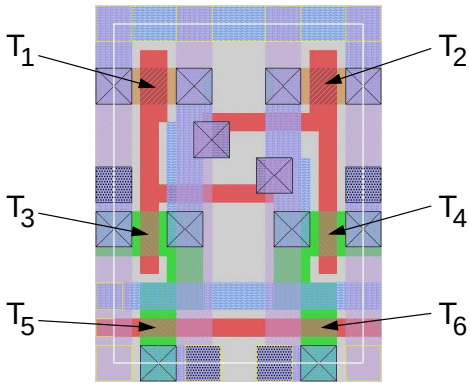

Рис.2. Топология ячейки статического ОЗУ

Если транзистор T_3 удастся приоткрыть на очень короткое время внешним воздействием, то это может привести к изменению состояния триггера. Воздействуя на транзистор T_4, состояние триггера может быть изменено на противоположное. Основная сложность, которая может возникнуть, это фокусировка ионизирующего излучения в области нескольких мкм^2 и выбор необходимой интенсивности излучения.

3 Эксперимент

Для наших экспериментов мы выбрали стандартный микроконтроллер PIC16F84, который содержит на кристалле 68 байт статического ОЗУ (Рис.3). К нему мы применили стандартную операцию распаковки и ее результаты показаны на Рис.4. Матрица ОЗУ расположена в середине нижней части кристалла и с 80-кратным увеличением показана на Рис.5.

Рис.3. Микроконтроллер PIC16F84

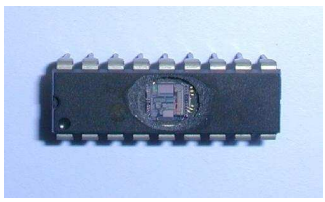

Рис.4. Распакованный PIC16F84

Поскольку наш бюджет был довольно сильно ограничен, а то лазерное оборудование которым мы располагали оказалось неприемлемо для наших экспериментов, мы решили использовать недорогую фотовспышку (Vivitar 550FD, б/у, купленную за 30 долларов в фотомагазине). Хотя яркость фотовспышки гораздо меньше, чем у импульсного лазера, при соответствующем увеличении можно достичь требуемого уровня ионизации. Мы закрепили фотовспышку при помощи изоленты на видеопорту имеющейся у нас ручной станции микропробинга Wentworth Labs MP-901 (Рис.6). Увеличение было установлено на максимум – 1500х.

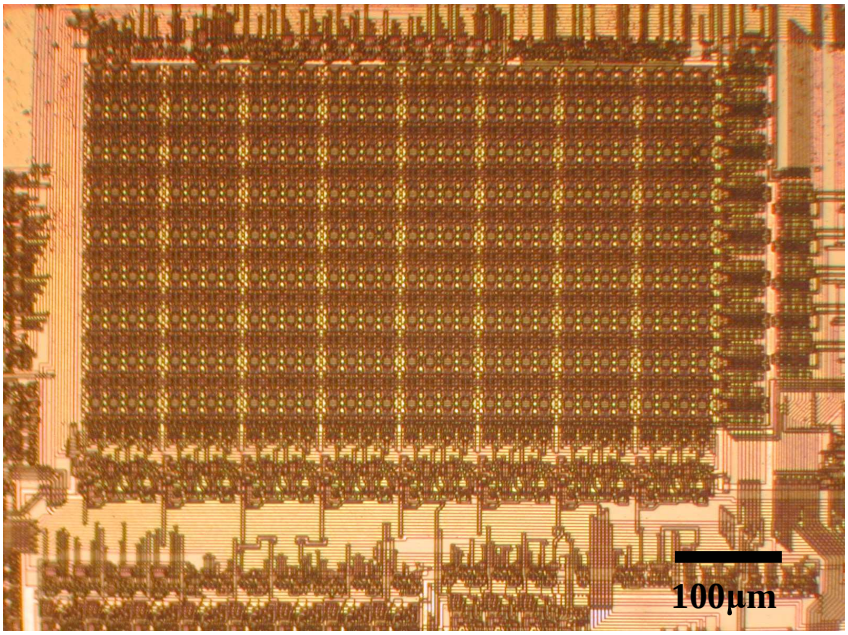

Рис.5. Матрица статического ОЗУ под микроскопом

Микроконтроллер был запрограммирован таким образом, что можно было с компьютера загружать и выгружать содержимое его ОЗУ. Заполняя всю память постоянными величинами, воздействуя фотовспышкой и затем выгружая содержимое памяти, мы могли наблюдать какие ячейки изменили свое значение.

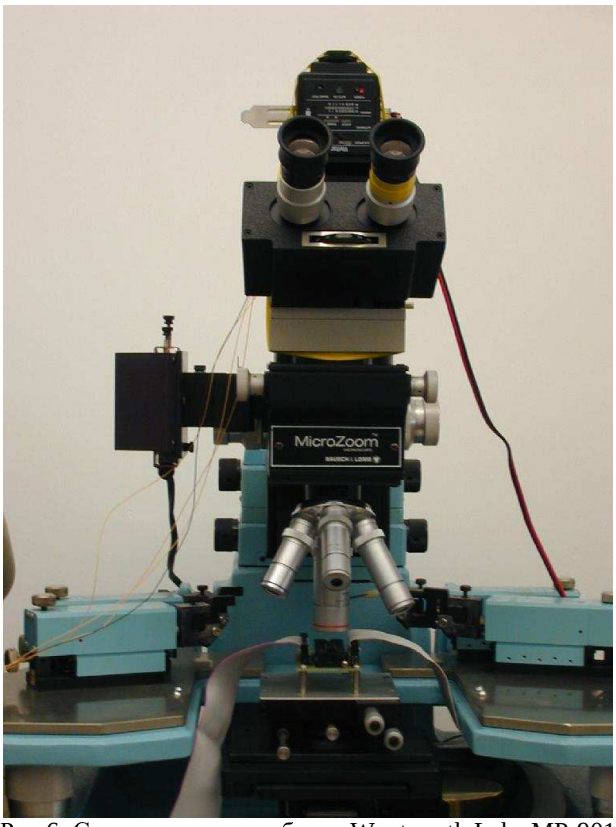

Рис.6. Станция микропробинга Wentworth Labs MP-901
с прикрепленной к ней фотовспышкой Vivitar 550FD

4 Результаты

Мы смогли устанавливать в требуемое состояние любой отдельный бит в статическом ОЗУ. Область ОЗУ при максимальном увеличении показана на Рис.7. Фокусировка света от фотовспышки на облась ограниченную белой окружностью, вызывала переключение ячейки из состояния лог.1 в состояние лог.0 или никаких изменений, если ячейка была в состоянии 0. Фокусировка света на область, показанную черной окружностью, вызывала переход ячейки из 0 в 1 или никаких изменений, если она уже была в 1.

На Рис.5 отчетливо видно, что матрица ОЗУ разделена на восемь одинаковых областей. Облучая ячейки из разных областей, мы обнаружили, что каждая область соответствует отдельному биту

данных в информации (Рис.8).

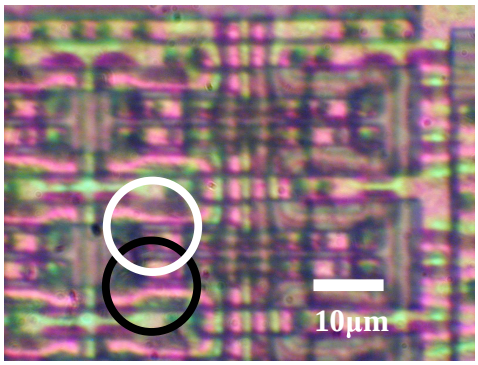

Рис.7. Матрица статического ОЗУ при максимальном увеличении

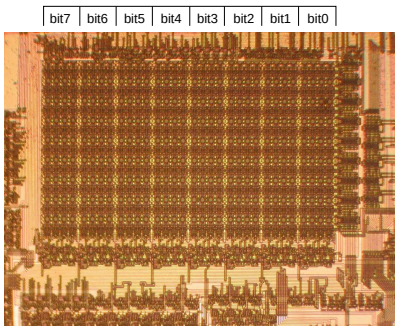

Рис.8. Расположение битов данных в матрице ОЗУ в PIC16F84

Путем последовательного облучения каждой ячейки в блоке мы построили карту адресов памяти соответствующих физическому положению каждой ячейки в блоке. Результат показан на Рис.9, при этом левый край соответствует нижнему краю блока. Можно также заметить, что адреса располагаются не последовательно, а разделены на три группы.

30h	34h	38h	3Ch	40h	44h	48h	4Ch	10h	14h	18h	1Ch	20h	24h	28h	2Ch	0Ch
31h	35h	39h	3Dh	41h	45h	49h	4Dh	11h	15h	19h	1Dh	21h	25h	29h	2Dh	0Dh
32h	36h	3Ah	3Eh	42h	46h	4Ah	4Eh	12h	16h	1Ah	1Eh	22h	26h	2Ah	2Eh	0Eh
33h	37h	3Bh	3Fh	43h	47h	4Bh	4Fh	13h	17h	1Bh	1Fh	23h	27h	2Bh	2Fh	0Fh

Рис.9. Расположение адресов в каждом блоке ОЗУ в PIC16F84

Это показывает как легко полуинвазивные атаки могут быть использованы для реинжиниринга карты памяти. Единственное ограничение это то, что фотовспышка не дает равномерный и монохроматический свет, т.е. очень трудно контролировать область воздействия излучения. Однако эта проблема может быть решена при переходе к подходящему лазеру.

5 Сложности и дальнейшая работа

Эта работа показывает каким образом оптические атаки можно провести используя недорогое оборудование. Мы повторили наши

эксперименты, используя лазерную указку (Рис.10), купленную за 8 долларов, и управляемый координатный столик. Мы достигли тех же результатов за исключением некоторых практических деталей. С одной стороны, мы смогли тестировать поверхность чипа автоматически и со скоростью до 100 вспышек в секунду. С другой стороны, мы должны были более тщательно позиционировать чип из-за меньшей зоны фокусировки и слабой мощности лазера. Лазерная указка является лазерным устройством Класса II (<1мВт), но мы увеличили ток на драйвере таким образом, что выходная мощность должна была достичь 10мВт. Мы смогли сфокусировать луч на поверхности чипа до пятна в 1мкм и длина волны излучения была около 650нм.

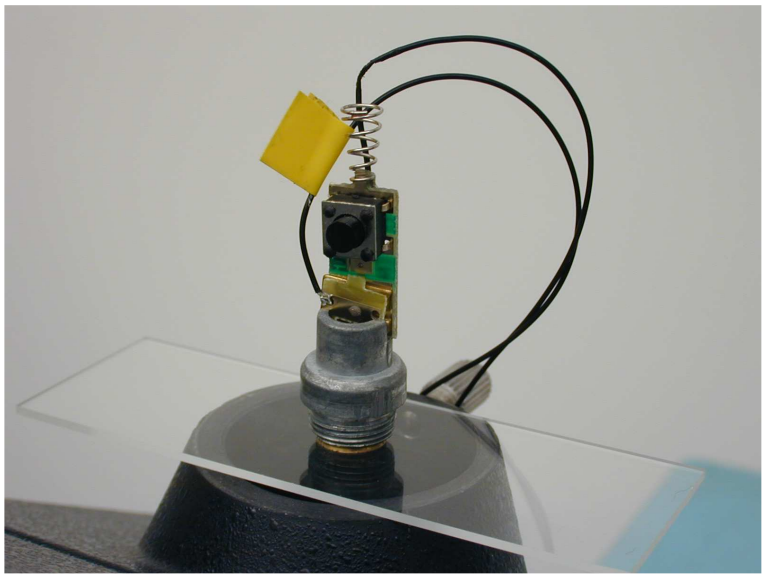

Рис.10. Лазерная указка установленная на видеопорт микроскопа

Мы использовали наше автоматизированное оборудование для проведения атак на различные полупроводниковые устройства. Лучшие образцы современных защищенных микроконтроллеров не подвержены атакам при помощи одиночные лазерных вспышек. Однако ряд устройств может быть взломан путем изменения состояния триггера, который содержит бит защиты. Мы настойчиво рекомендуем, чтобы разработчики интегральных схем изучали свой

дизайн на предмет отсутствия возможности сбоя защиты при ошибке в одном транзисторе.

Атаки также были проведены на смарткартах. На данном этапе было бы полезно вспомнить раннюю литературу по анализу сбоев. В [1] Бонех (Boneh), Демилло (Demillo) и Липтон (Lipton) выявили, что неправильный расчет цифровой подписи RSA приводит к утечке ключа подписи. Например, секретный расчет $S = h(m)^d \pmod{pq}$ проводится как $\bmod p$, затем $\bmod q$, и потом результат комбинируется, поскольку это значительно быстрее. Однако если смарткарта возвращает неправильную величину S_p, которая корректна по модулю p, но некорректна по модулю q, то можно восстановить $p = \gcd(pq, S_p^e - h(m))$.

В [2], Андерсон (Anderson) и Кун (Kuhn) указали на то, что вмешательство в инструкции перехода процессора является более мощной и основной атакой: взломщик, который может вызвать ошибку в условном переходе при исполнении программного кода в смарткарте и, например, уменьшить число циклов в шифровании, сделает извлечение секретного ключа достаточно простой задачей. Первая из описанных выше атак была успешно проведена, используя нашу технологию, однако договор с производителем не позволяет нам давать какие-либо детали.

Дальнейшие планы нашей научной работы предполагают исследования потенциала для атак при использовании хорошо оснащенной лаборатории, под которой мы понимаем современную станцию микропробинга с многоволновым режущим лазером. Мы арендуем такое оборудование и планируем его использовать для исследования возможности атак с обратной стороны чипа при помощи ИК излучения. Мы также получили доступ к подходящему источнику рентгеновского излучения и исследуем как оно может быть использовано для внесения ошибок в работу устройств. Важность этого состоит в том, что рентгеновское излучение может проникать сквозь верхние слои металлизации, также как и через большинство защитных упаковок, используемых на практике.

6 Защита

Описанные выше оптические атаки являются новой мощной технологией для атак на смарткарты и другие защищенные процессоры. Мы предвидим, что подобно анализу потребляемой

мощности предложенному Кочером (Kocher) в [10], они могут иметь значительный коммерческий эффект для индустрии в том, что потребуют тщательной переоценки требований безопасности и введения новых технологий защиты.

Следуя тем же путем, мы решили задержать аннонсирование наших атак до тех пор, пока не будут доступны достойные методы защиты. Существующие современные технологии защиты, такие как защитные верхние слои металлизации и шифрование шины данных, могут затруднить атаки, но не полностью их исключить. Изощренный взломщик может обойти защитную металлизацию используя инфракрасный свет или ренгеновское излучение, тогда как зашифрованная шина данных может быть обойдена прямой атакой на регистры.

Защитная технология, которую мы разработали, использует самотактируемую двухпроводную логику. Обычная цифровая логика использует тактовый сигнал для синхронизации; но по мере того, как устройства становятся все сложнее и сложнее становится все труднее увеличивать тактовую частоту, и это привело к разработке самотактируемых, или асинхронных, схем – схем, которые не используют тактовый сигнал. Такие схемы требуют механизм, посредством которого функциональные компоненты в схеме могут сигнализировать что они готовы к принятию данных или уже приняли их. Один из таких путей – это использование задержек в пути данных.

В двухпроводной логике 0 или 1 кодируются не высоким или низким напряжением на одной линии, а комбинацией сигналов на паре линий. Например, 0 может быть ‘LH’, а 1 может быть ‘HL’. При использовании в самотактируемой логике, ‘LL’ сигнализирует готовность. Основной недостаток такого простого распределения это низкая надежность: ошибки приводят к появлению ненужного состояния ‘HH’, которое быстро распространяется по всей схеме и блокирует ее работу.

Наше новшество состояло в использовании этой низкой надежности как преимущество, делая состояние ‘HH’ как сигнал ошибки. Этот сигнал может быть возведен намеренно детектором проникновения, вызывая блокировку устройства [11]. Наибольший интерес представляет то, что одиночные ошибки не смогут вызывать утечку важной информации [12]. Мы верим, что подобные требования

будут предъявляться в будущем к устройствам с высоким уровнем защиты.

Инженерные детали не являются тривиальными. Например, очевидная озабоченность тем, что почти любая незамеченная ошибка в RSA подписях может быть использована в атаках по Бонеху. В связи с этим наши коллегги разработали модульный умножитель, используя нашу технологию. Аналогично, хотя шифрование шины данных устраняет необходимость защищать область памяти, остается риск атаки на счетчик адреса и регистры. Поэтому другие наши коллеги разработали регистры и устройство управления памятью использующие нашу технологию [11].

7 Заключение

Стандартные КМОП схемы очень чувствительны к оптическим атакам. Воздействуя на транзистор лучом лазера или даже сфокусированным светом от фотовспышки, можно заставить его проводить ток. Это дает много возможностей для атак. Мы в деталях описали как воздействуя ярким светом на определенную область ячейки статического ОЗУ можно изменять ее состояние. Другими технологиями памяти, такими как УФППЗУ (EPROM), ЭППЗУ (EEPROM) и флэш-память (FLASH), также возможно манипулировать различными способами.

Однако, это только начало. Обладая достаточно дорогим оборудованием взломщик может внести ошибку в работу любого транзистора в КМОП схеме в требуемый момент времени. Это будет иметь сокрушительные последствия для защиты. Поэтому необходимы противодействия этому на уровне дизайна схемы.

Литература

[1] D. Boneh, R. A. DeMillo, R. J. Lipton, “On the Importance of Checking Cryptographic Protocols for Faults, Advances in Cryptology – Eurocrypt 97”, Springer LNCS vol 1233 pp 37–51

[2] R. J. Anderson, Markus G. Kuhn, “Low Cost Attacks on Tamper Resistant Devices”, in M.Lomas et al. (ed.), Security Protocols, 5th International Workshop, Paris, France, April 7-9, 1997

[3] R. J. Anderson, “Security Engineering – A Guide to Building Dependable Distributed Systems”, Wiley 2001

[4] J. J. Quisquater, D. Samyde, “ElectroMagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards”, International Conference on Research in Smart Cards, E-smart 2001, Cannes, France, pp 200–210, Sept. 2001

[5] D.H. Habing, “Use of Laser to Simulate Radiation-induced Transients In Semiconductors and Circuits”, IEEE Trans. Nuc. Sci., Vol NS-12, No 6, pp 91–100, Dec. 1965

[6] A.H. Johnston, “Charge Generation and Collection in p-n Junctions Excited with Pulsed Infrared Lasers”, IEEE Trans. Nuc. Sci., Vol NS-40, No 6, pp 1694–1702, 1993

[7] “Handbook of Optical Constants of Solids”, edited by Edward D. Palik, Orlando: Academic Press, 1985, pp 547–569

[8] J. M. Rabaey, “Digital Integrated Circuits: A Design Perspective”, Prentice-Hall, 1995

[9] K. Yun, “Memory”, UC San Diego, Adapted from EE271 notes, Stanford University

[10] P. Kocher, “Differential Power Analysis”, Advances in Cryptology – Crypto 99, Springer LNCS vol 1666 pp 388–397

[11] S. W. Moore, R. J. Anderson, M. G. Kuhn, “Improving Smartcard Security using Self-Timed Circuit Technology”, Fourth AciD-WG Workshop, Grenoble, ISBN 2-913329-44-6, 2000

[12] S. W. Moore, R. J. Anderson, P. Cunningham, R. Mullins, G. Taylor, “Improving Smartcard Security using Self-Timed Circuits”, Asynch 2002, proceedings published by IEEE Computer Society Press