УЯЗВИМОСТЬ FLASH NAND

Цыбулько К.Д.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Заливако С.С. – канд. тех. наук

В статье освещается проблема хранения информации на NAND-флэш носителях. Рассматриваются проблемы, связанные с возникновением различного рода ошибок и уязвимостей, а также пути их сглаживания и устранения.

За последние годы накопители информации на основе NAND-флэш памяти (структурная схема приведена на рис. 1) стали доминирующими в электронных устройствах различного назначения (USB-флэш накопители, карты памяти различных типов, мобильные устройства, такие, как телефоны, фотоаппараты, медиаплееры и др.). NAND-флэш - это форма энергонезависимой памяти (Electrically Erasable Programmable Read-Only Memory, EEPROM), которая может быть электрически стерта и записана. Накопитель состоит из массива элементов флэш-памяти и контроллера, который обрабатывает запросы на чтение или запись данных и, таким образом, представляет собой интерфейс между флэш-памятью и хостом. Основными причинами широкого распространения NAND-флэш является то, что ее емкость постоянно растет, а стоимость (количество бит на цент) уменьшается. Такой эффект является результатом двух тенденций: эффективного масштабирования технологических процессов и многоуровневого кодирования ячеек (multi-level cell, MLC; triple-level cell, TLC; qual-level cell, QLC) [1]. С другой стороны, становится все труднее обеспечивать надежность хранения данных во флэш-памяти. Указанные выше тенденции приводят к уменьшению количества электронов в транзисторе с плавающим затвором и усилению взаимного влияния элементов памяти.

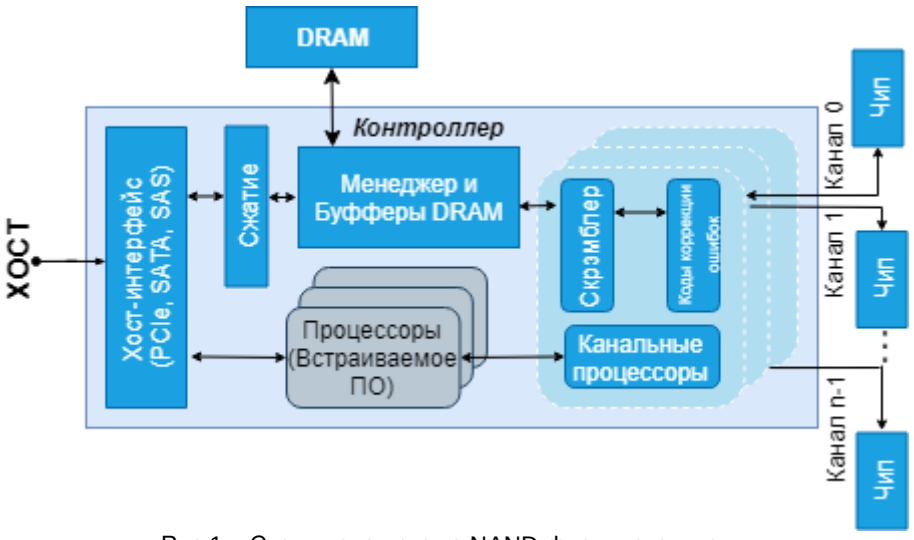

Рис.1 – Структурная схема NAND-флэш накопителя

Возникновение ошибок во флэш-памяти во многом зависит от данных, хранящихся в ячейках, и от работы различных приложений. Для уменьшения зависимости частоты ошибок от данных и предотвращения записи данных вредоносными приложениями, контроллер скремблирует (scrambling) данные перед записью. Основная концепция скремблирования заключается в генерации псевдослучайной последовательности нулей и единиц, для того чтобы минимизировать любые ошибки, которые зависят от данных. Реализация скремблирования приведена на рис. 2 и выполняется с использованием линейного сдвигового регистра с обратной связью (Linear Feedback Shift Register, LFSR). Так как скремблирование и дескремблирование с помощью LFSR реализуются одинаково (за счет свойств операции XOR), для корректного выполнения дескремблирования необходимо только знание начального состояния регистра [2]. В связи с этим для каждой записываемой страницы данных в качестве начального состояния LFSR может использоваться логический адрес этой страницы (таким образом, страница может быть правильно дескремблированна, даже если операции обслуживания переносят страницу в другое физическое местоположение). Однако, стоит отметить, что вредоносное приложение может обойти скремблирование. Злоумышленник воссоздает скремблер в программном обеспечении, которое имитирует его работу. Поскольку все необходимые составляющие для скремблирования известны (логический адрес страницы и неприводимый полином для LFSR), дескремблированные данные из вредоносной программы могут быть записаны в SSD.

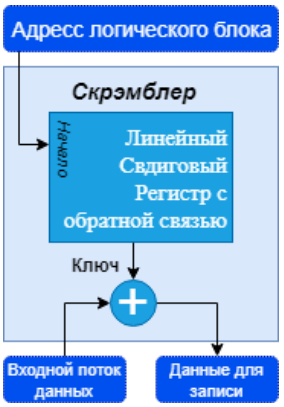

Рис.2 – Структурная схема скремблера

Помимо вредоносного программного обеспечения флэш-память подвержена случайным ошибкам. Есть два основных источника таких ошибок. Они возникают в частично запрограммированных ячейках памяти. Первым источником ошибок является результат взаимного влияния программ, приводящее к тому, что пороговое напряжение ячейки увеличивается при программировании соседней. Второй тип ошибок возникает при чтении. Оно приводит к существенному сдвигу порогового напряжения для ячейки с более низким напряжением. Таким образом, незапрограммированные и частично запрограммированные ячейки будут сильнее подвержены такого рода ошибкам, так как они имеют более низкие пороговые напряжения.

Ошибки могут быть использованы вредоносными программами для повреждения данных. Есть

две модели использования ошибок: на основе межпрограммной интерференции между ячейками и возникновении ошибок при чтении [3]. Идея модели, основанной на межпрограммной интерференции, состоит в том, что вредоносное приложение может вызывать множество ошибок на странице другого приложения, тем самым разрушая страницу и сокращая срок службы SSD. Целью первой модели является запись вредоносным приложением наихудшей комбинации данных (например, все нули) на страницу таким образом, чтобы вызвать максимальное количество программных ошибок. Модель нарушения чтения использует тот факт, что двухэтапное программирование значительно повышает уязвимость как частично запрограммированных, так и незапрограммированных элементов флеш-памяти. Механизм работы второй модели заключается в том, что вредоносное приложение быстро выполняет большое количество операций чтения за очень короткий промежуток времени, тем самым, вызывая ошибки при чтении, которые повреждают частично запрограммированные страницы. В данной модели вредоносному приложению не нужно иметь дополнительной информации об атакуемом приложении. Так же, программа может атаковать сразу несколько страниц флэш-памяти, и повреждать страницы, записанные после совершения атаки.

В настоящее время применяются следующие решения для устранения описанных выше атак: буферизация данных DRAM в контроллере, адаптивное считывание опорного напряжения и использование нескольких проходных напряжений [4]. Последние два решения устраняют от 20% до 70% возникающих ошибок и могут быть использованы не для всех типов атак. Самым эффективным решением, согласно [4], является буферизация данных в контроллере, которая полностью устраняет возникающие ошибки при чтении данных и межпрограммной интерференции. Однако вызывает задержку от 1% до 16% при чтении данных и требует дополнительной памяти до 2 Мб. Таким образом, издержки наисправления значительно увеличиваются. Для повышения надежности NAND-флэш памяти необходимо пересмотреть существующие решения, в том числе связанные с равномерной записью информации и добавлением к контроллеру детектора напряжения.

Равномерная запись информации позволит уменьшить изнашиваемость с помощью перераспределения информации по всем элементам памяти, увеличивая тем самым общий срок службы устройства. Детектор напряжения будет блокировать операции с флэш-памятью при выходе питающего напряжения за допустимые границы, тем самым позволяя избежать ошибок связанных с взаимодействием между элементами памяти. Данный метод будет почти со 100% вероятностью устранять ошибки связанные с взаимодействием между элементами памяти, однако метод будет требовать дополнительный аппаратуры и, соответственно, стоимость накопителя повысится.

Список использованных источников:

1. Yu Cai, Saugata Ghose, Erich F. Haratsch, Yixin Luo, Onur Mutlu/ Error Characterization, Mitigation and Recovery in Flash-Memory-Based Solid-State Drives (Proceedings of the IEEE, September2017);
2. J.P. van Zandwijk /A mathematical approach to NAND falsf-memory descrambling and decoding /Digital Investigation 12 (2015) 41e5242
3. Yu Cai, Saugata Ghose, Erich F. Haratsch, Yixin Luo, Onur Mutl/ Vulnerabilities in MLC NAND Flash Memory Programming: Experimental Analysis,Exploits,and Mitigation Techniques;
4. Y. Cai et al., “Characterization and Mitigation of Reliability and Security Vulnerabilities in MLC NAND Flash Memory Programming,” Carnegie Mellon Univ., SAFARI Research Group,Tech.Rep.2017-002,2017.