Транслятор файловой системы для SD-карт

ТАТЬЯНА ЛУКОЯНОВА, инженер 1 категории, ЗАО «ПКК Миландр»
ВАЛЕРИЙ МАЛЫХ, директор представительства, ЗАО «ПКК Миландр» (Нижний Новогород)

В статье рассказывается о новой разработке «ПКК Миландр» — высокоскоростных криптографических микроэлектронных SD-картах, обеспечивающих надежную защиту данных.

Компания «ПКК Миландр» разработала принципы и структуру энергоэффективных высокоскоростных криптографических микроэлектронных карт в форм-факторах SD и miniSD в соответствии со спецификацией SDv.2.0. Разработка позволяет решить проблемы в области защиты данных. Во-первых, речь идет о защите данных личного плана. Широкое распространение индивидуальных мобильных устройств — смартфонов, планшетов, коммуникаторов, использование корпоративных ресурсов, почтовых программ и онлайн-банкингов вынуждает нас пользоваться паролями, которые должны периодически меняться. Хранение такого количества непростых символьных данных становится нетривиальной задачей. Во-вторых, пользователю предоставляется собственный инструмент для формирования способов и алгоритмов защиты, которые хранятся в памяти и при необходимости корректируются. Таким образом, вместо доступа к корпоративным ресурсам (включая электронную почту) по паролю, для входа в домен можно использовать аппаратную аутентификацию и защиту электронной переписки в сетях, построенных на базе ОС Windows. В данной конструкции в качестве носителей ключевой информации используются электронные идентификаторы и специализированное приложение.

ОСНОВНОЙ АЛГОРИТМ

Приоритетными задачами обеспечения безопасности корпоративных ресурсов являются авторизация пользователей (вход в домен при подключении карты и блокирование сессии после ее отсоединения), электронная цифровая подпись почтовых сообщений и их шифрование, доступ к корпоративным сетям, онлайн-ресурсам банков (финансовых организаций) по предъявлении электронного ключа, надежное хранение и использование сертификатов.

В настоящее время широкое распространение получили персональные средства аутентификации и защищенного хранения данных, аппаратно поддерживающие работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП). Они выпускаются в основном в форм-факторах USB-ключа и смарт-карт. Подобные устройства удобно использовать на стационарных ПК, но в мобильных устройствах связи — смартфонах, коммуникаторах, планшетах USB-входы отсутствуют, производители ограничиваются SD-входом. Разработка «ПКК Миландр» позволила отработать основные алгоритмы и конструкцию микроэлектронного изделия в форм-факторе SD-карты и miniSD-карты. Структурная схема изделия представлена на рисунке 1.

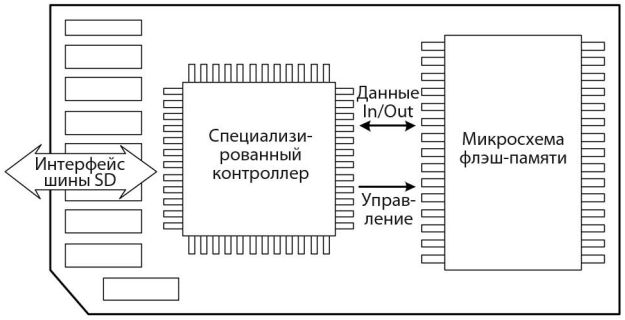

Рис. 1. ***Структурная схема микроэлектронной SD-карты***

КОНСТРУКЦИЯ ИЗДЕЛИЯ

Конструктивно изделие состоит из микроконтроллера (МК) и элемента памяти типа NAND-флэш. МК управляет интерфейсом SD-карт в режиме ведомого устройства в соответствии со спецификацией SDv2.0, контролирует хранение массивов информации в энергонезависимой памяти, выполняет программную поддержку специальных криптографических алгоритмов. Со стороны хоста обменом управляет специальное приложение, без которого изделие определяется в системе как обычная карта памяти. Структурная схема МК представлена на рисунке 2.

МК с набором периферийных модулей объединен общей шиной InternalBus. Выполнение криптографических функций возложено на ядро Cryptocore. Контроллер выполнен на основе высокопроизводительного 32-разрядного процессорного RISC-ядра Cortex M1.

В состав МК входят:

- контроллер интерфейса NAND-флэш (скорость не менее 1 Мбайт/с);
- ОЗУ данных (RAM DATA) емкостью 32 Кбайта;
- ЭСППЗУ памяти программ (EEPROM Program) емкостью 64 Кбайта;
- ЭСППЗУ памяти данных (EEPROM DATA) емкостью 512 байт;
- контроллер интерфейса SD-карт обеспечивает работу в режимах memorySD и SDIO в соответствии со спецификацией SD v2.0 (скорость обмена не менее 1 Мбайт/с);
- память емкостью 128 Кбайт и ОЗУ емкостью 48 Кбайт для хранения программ и данных;
- криптографическое ядро аппаратно реализует генерацию ключей ЭЦП и формирование ЭЦП по стандарту ГОСТ Р 34.10-2001, а также преобразование данных в

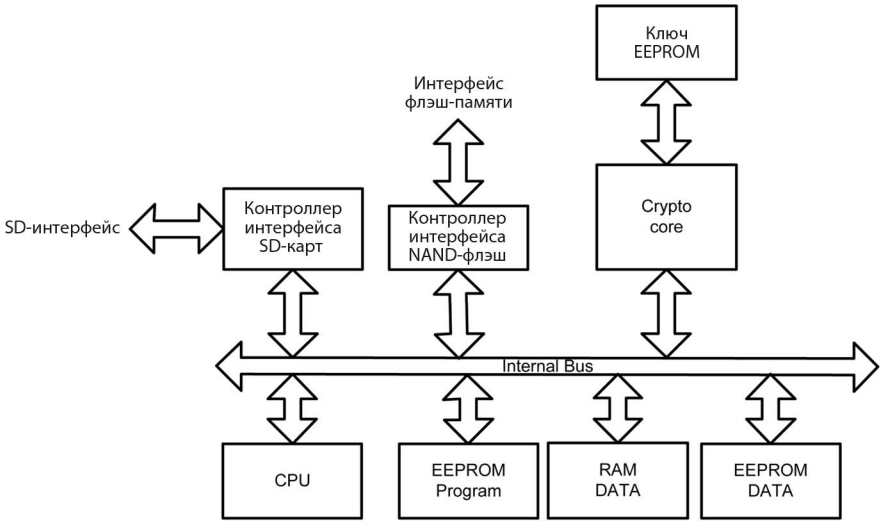

Рис. 2. ***Структурная схема микроконтроллера***

соответствии с отечественным стандартом шифрования ГОСТ 28147-89.

Изделие в форм-факторе SD-карты и miniSD-карты обеспечивает функционирование в следующих режимах:

- режим SD-карты (тип memorySD) в соответствии со спецификацией SDcardv 2.0;
- аутентификация пользователя, аутентификация изделия, взаимная аутентификация изделия и хост-устройства;
- установка режима шифрования/расшифрования;
- режим шифрования/расшифрования данных во встроенной памяти по ГОСТ 28147-89;
- режим шифрования/расшифрования данных на проходе по ГОСТ 28147-89;
- формирование и проверка ЭЦП по ГОСТ Р 34.10-2001;
- технологический (отладочный) режим блокируется перед поставкой конечному пользователю.

Обмен между хостом и картами управляется хостом. В соответствии со спецификацией SD хост посылает команды двух типов: широковещательные и адресованные (двухточечные) команды. Широковещательные команды предназначены для всех карт. Адресованные команды предназначены одной карте. Некоторые из этих команд требуют ответа.

Есть четыре вида определенных команд, чтобы управлять картой памяти SD:
- широковещательные команды без передачи ответа (bc);
- широковещательные команды с передачей ответа (bcr);
- адресованные (двухточечные) команды без передачи ответа (ac);
- адресованные (двухточечные) команды с передачей ответа (adtc).

Согласно требованиям спецификации SD SpecificationVersion 2.0 для обеспечения работы по шине SD устройство должно обеспечивать:
- прием и определение номера команды от хоста;
- отправку ответов на принятую команду (передача текущего состояния карты, данных);
- выполнение диаграммы переходов состояний SD-устройства;
- выполнение операций последовательного чтения блоков;
- выполнение операций последовательной записи блоков.

При использовании флэш-памяти в качестве носителя информации контроллер должен интерпретировать ее как блочное устройство, которое позволяет записывать и читать блоки данных установленного размера в виде сектора диска. Это, в свою очередь, позволяет стандартизировать файловые системы, спроектированные для магнитных дисков, такие как FAT, для использования устройств флэш. В такой постановке код файловой системы называется драйвером устройства, поддерживающим запросы операции записи и чтения. Драйвер устройства сохраняет и восстанавливает блоки устройства флэш.

Однако при отображении блоков на адреса флэш простым линейным видом возникают две проблемы. Во-первых, одни блоки данных могут быть записаны намного больше раз, чем другие. Это не представляет проблемы для магнитных дисков, т.к. обычные файловые системы не пытаются избегать таких ситуаций. Но когда файловая система отображается на устройство флэш, некоторые блоки стираются чаще, соответственно замедляется доступ по времени, что в конечном счете приводит к выходу блока из строя. Эта проблема может быть решена при использовании более сложной схемы отображения и перемещения блоков. Подобные методики называют выравнивающими изнашивание методиками.

Второй проблемой, которая создается в результате отображения тождественности, является неспособность записывать блоки данных меньшего объема, чем у модуля стирания устройства флэш. Предположим, что блоки данных, используемые файловой системой, составляют 4 Кбайта каждый, а модули стирания — 128 Кбайт каждый. Если блоки 4 Кбайта отображены на адреса флэш с использованием отображения тождественности, то запись блока 4 Кбайта потребует копирования модуля стирания 128 Кбайт в ОЗУ, записи измененной области 4 Кбайта, стирания модуля стирания и перезаписи из ОЗУ. Кроме того, если отключение питания произошло прежде, чем весь модуль стирания перезаписан в устройство флэш, то 128 Кбайт данных будут потеряны. В магнитном диске мог быть потерян блок 4 Кбайта. Оказывается, что выравнивающая изнашивание методика автоматически обращается к этой проблеме.

Для решения возникших проблем был разработан собственный драйвер файловой системы. Основная идея драйвера состоит в том, чтобы отобразить номер блока, представленный хостом (логический адрес), к физическому адресу флэш. Создается карта соответствия логических и физических секторов. Когда виртуальный блок должен быть перезаписан, новые данные не переписывают в физический блок, где он в настоящее время сохраняется. Вместо этого новые данные записываются в другой физический блок, и карта «логический блок — физический блок» обновляется. Старая копия логического блока продолжает храниться на флэш, но должна быть помечена как устаревшая. Следовательно и последняя записанная (достоверная) копия логического блока должна быть помечена соответствующим образом. Когда производится чтение блока, система, основываясь на карте соответствия, находит физический блок.

Как правило, сектора имеют установленный размер и занимают фрагмент модуля стирания. В устройствах типа NAND сектора обычно занимают одну флэш-страницу. Но в устройствах типа NOR тоже можно использовать сектора переменной длины. Такое отображение отвечает нескольким целям. Во-первых, при записи часто изменяемых блоков в различные сектора в каждой модификации отображение выравнивает изнашивание различных модулей стирания. Во-вторых, отображение позволяет записывать отдельный блок во флэш, не стирая и не перезаписывая весь модуль стирания. В-третьих, отображение позволяет осуществлять запись блока атомарно так, чтобы если питание было отключено во время операции записи, блок возвращался в состояние предварительной записи, когда флэш будет использоваться снова.

Во время работы устройство флэш будет накапливать устаревшие сектора, и количество свободных секторов будет уменьшаться. Чтобы освободить пространство для новых и обновления хранимых секторов, устаревшие сектора должны быть удалены. Это называется восстановлением модуля стирания или «сборкой мусора». Восстановление может выполняться в любое время, когда центральный процессор простаивает, или по требованию, когда количество свободного пространства понижается ниже предопределенного порога. Таким образом, каждый физический блок флэш и модуль стирания в целом имеют информационную структуру, которая определяет текущее состояние модуля стирания.

На основании этой информации, хранимой во флэш, система строит карту «логический блок — физический блок». Эта карта хранится частично в ОЗУ. Причина, по которой карта хранится в ОЗУ, состоит в том, что оно поддерживает быстрый поиск и обновление. Имеется в виду, что в случае, когда логический блок перезаписан и перемещен от одного физического блока к другому, местоположение поиска должно быть обновлено. Флэш не поддерживает такой оперативной модификации.

Вторая необходимая таблица, которая хранится в ОЗУ, содержит информацию о модулях стирания, а также о количестве достоверных, устаревших, свободных модулей. Таким образом, в программе драйвера файловой системы были реализованы следующие процедуры:
- чтение логического блока;
- запись логического блока;
- поиск свободного места для записи;
- восстановление модуля стирания;
- формирование и обновление карты «логический блок — физический блок»;
- формирование и обновление таблицы «информация о модулях стирания».

Учитывалось и то, что кроме работы в режиме memorySD данное изделие предусматривает также режимы, направленные на криптографические преобразования

данных. Это потребовало введения дополнительного (относительно спецификации SD карт v2.0) набора команд. Основные назначения команд — выполнение процедур аутентификации пользователя, изделия и хоста, формирование и проверка ЭЦП, выполнение процедур шифрования и расшифрования.

Доступ пользователя к функциям криптографической обработки информации разрешается после аутентификации изделия или взаимной аутентификации изделия и хост-устройства. Режим аутентификации выбирается в зависимости от условий и целей использования изделия. Изначально пользователь предъявляет пароль, смена пароля возможна только после предъявления предыдущего пароля. Исходный пароль доступа вводится в изделие при изготовлении и сообщается конечному пользователю. Механизм доступа по паролю соответствует операции блокировки/разблокировки карты согласно спецификации SDv2.0. После прохождения процедуры аутентификации пользователя хост и изделие проводят процедуру взаимной аутентификации. В случае успеха приложение предоставляет пользователю доступ к своим криптографическим возможностям.

Макетирование на ПЛИС позволило согласовать и отладить программные и аппаратные составляющие изделия. В результате на макете были получены следующие характеристики:

- скорость чтения данных 1,7 Мбайт/с;
- скорость записи данных 1,5 Мбайт/с;
- объем памяти для хранения данных 4 Гбайт (полезный объем 3,4 Гбайт).

Расширение функций изделия будет возможно при разработке генератора случайных паролей, при поддержке нескольких алгоритмов шифрования и формирования ЭЦП, а также за счет расширения возможностей приложения, увеличения скорости работы и выполнения изделия в форм-факторе microSD.

ВЫВОДЫ

Изделие будет выполнено в виде одной микросхемы и позволит решить следующие задачи:

- усовершенствовать процесс аутентификации (двухфакторная аутентификация) на локальном компьютере и в корпоративной сети и обеспечить защищенный доступ к бизнес-приложениям;
- защитить программное обеспечение от нелицензионного использования и копирования;
- зашифровать данные на серверах, ноутбуках и рабочих станциях;
- обеспечить защиту персональных данных;
- защитить электронную почту и взаимодействие с коллегами в системах электронного документооборота;
- обезопасить финансовые операции в системах дистанционного банковского обслуживания;
- внедрить электронную цифровую подпись и защитить документы в системах сдачи электронной отчетности через интернет;
- обеспечить защиту корпоративного сайта в интернете;
- обезопасить себя от кражи паролей к онлайн-сервисам (Web-money и др.) и социальным сетям («Одноклассники», «ВКонтакте» и др.).

Преимуществом данного изделия является его малый форм-фактор, что позволяет решать перечисленные задачи при использовании стационарных ПК, ноутбуков, смартфонов, коммуникаторов, КПК, планшетных ПК, т.е. везде, где поддерживаются SD-карты.