СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Одним из примеров интереснейшего применения электроники в конце XX столетия является чип-карта, изобретение которой в некоторой степени изменило жизнь каждого из нас. Для всех обыкновенных людей чип-карта – своего рода «сезам», который окружен тайнами и загадками и постепенно начинает заменять ключи и деньги.

Для специалиста по электронике чип-карта, помимо всего прочего, – неисчерпаемый повод для экспериментов, хотя бы потому, что это обычное семейство электронных компонентов самого широкого применения, которое можно вполне законно изучать и применять. К тому же сроки действия основных патентов закончились или заканчиваются в ближайшем будущем и один за другим становятся достоянием общества.

Теперь, после преодоления всех сомнений, по понятным причинам обуревавших разработчиков чип-карт, доказано, что не имеет смысла скрывать описания устройств для всевозможных типов электронных карточек, позволяющих считывать или записывать информацию.

Безопасность «электронных крепостей», которыми могут и должны быть карты, предназначенные для наиболее «тонких» сфер применения, основывается на специальных принципах и алгоритмах обработки информации, которые обеспечивают почти абсолютную защиту, если не допустить небрежности.

Ознакомившись с терминологией и со стандартами, действующими в сфере обращения электронных карт, вы научитесь производить чтение и запись данных в карты самых распространенных типов, а затем сможете приступить к практическому использованию чип-карт.

Автор желает своим читателям получить от работы с книгой и с рассмотренными в ней устройствами столько же удовольствия, сколько испытывает он сам, продолжая осваивать эту увлекательную отрасль современной электроники.

ВВОДНЫЕ ЗАМЕЧАНИЯ

Все схемы, приведенные в этой книге, были подготовлены на ЭВМ, совместимой с ПК, с установленным на ней программным обеспечением Boardmaker. Наши читатели интересуются этим продуктом, так как он не очень широко распространен. Прекрасно работающая версия этого ПО приведена на компакт-диске, который прилагается к книге автора "Logiciels PC pour l'electronique" (Программное обеспечение по электронике для ПК), вышедшей во Франции.[1] Таким образом, при желании можно изменить «оригинальную» координатную сетку, а затем перерисовать схему в выбранном масштабе. Автор выражает благодарность разработчикам Boardmaker за их любезное сотрудничество.

Искренняя благодарность выражается также компаниям Gemplus Card International, CNET de Caen (ранее SEPT), SGS-Thomson Microelectronics, Philips Semiconductors, Siemens, SEFEA, COREL Electronique, ITT-Cannon, Microchip, ATMEL и особенно всем тем, кто помог выполнить всю работу по подготовке книги.

Следует иметь в виду, что описываемые здесь схемы должны быть использованы только в экспериментах, но не в каких-либо коммерческих или промышленных целях. По всем вопросам, связанным с лицензированием патентов INNOVATRON, обращайтесь по адресу: INNOVATRON, rue Danton 1, 75006 PARIS.

[1] Издательство «ДМК» планирует выпустить русский перевод данной книги.

ГЛАВА СТРАНИЦА

1 ТЕРМИНЫ И СТАНДАРТЫ

Применительно к чип-картам разработана специфическая терминология (осмелимся сказать – своего рода жаргон), которую важно знать, чтобы расчитывать на понимание предмета. Главные участники нового «революционного движения в технике» под эгидой компетентных международных органов договорились завершить в скором времени разработку правил, гарантирующих удовлетворительный уровень совместимости карт различных типов, не препятствуя при этом постоянному развитию данной области электроники.

ЧТО ТАКОЕ ЧИП-КАРТА

На сегодняшний день чип-карта, или карта с интегральной микросхемой, – это пластина из полимерного материала, по размерам идентичная карте с магнитными полосами (например, кредитной). Нововведение состоит в возможности разместить в карте обыкновенной толщины одну или несколько интегральных микросхем и в применении переходной (соединительной) платы, способной обеспечить электрический контакт со специальным переходным (интерфейсным) устройством.

Микромодулем принято называть очень тонкую печатную плату, которую можно увидеть на поверхности чип-карты. На внешней стороне микромодуля расположены контактные площадки для подключения ко внешним устройствам; на внутренней стороне размещается кристалл микросхемы. Технология называется Chip on Board – кристалл на плате.

Так как вокруг микромодуля остается много свободного места, очевидно, что подобное техническое решение нельзя назвать оптимальным, поэтому ведется поиск новых вариантов конструкции. Уже появились такие «модифицированные» изделия – миниатюрные чип-карты.

Чип-карты часто отличают друг от друга по функциональному назначению микромодуля, иначе говоря, по их внутренним интегральным микросхемам. С учетом этого можно выделить три большие группы чип-карт:

- карты с простой памятью;
- карты с программируемой памятью;
- карты с микропроцессором.

КАРТЫ С ПАМЯТЬЮ

Карты с простой памятью

Как явствует из названия, такие карты обладают ограниченным количеством памяти без какой-либо особой защиты. Это означает, что каждый пользователь может считать или записать информацию в память с помощью некоторого устройства, которое можно совершенно свободно купить или просто изготовить своими силами. Эти вопросы будут рассмотрены далее.

Карты с простой памятью выполняются главным образом по технологии ЭСППЗУ и, следовательно, являются многоразовыми (возможны стирание и перезапись). Емкость подобных карт обычно составляет несколько килобитов, реже – несколько десятков килобитов. Такие устройства предназначены для применения в областях, не требующих особой защиты: несекретные статистические данные, картотеки, электронные технологические карты и др.

Карты с программируемой памятью

Чтобы заслужить название «чип-карта с программируемой памятью», электронная карта должна иметь как минимум четыре нижеописанные системы защиты, реализуемые логическими схемами, без помощи какого-либо микропроцессора:

- область памяти, защищаемая от записи разрушением плавкой перемычки;
- область памяти, защищаемая от чтения и записи «кодом пользователя» (этот конфиденциальный код называется также PIN-кодом, от Personal Identification Number – персональный идентификационный номер). Под словом «пользователь» подразумевается лицо, распоряжающееся чип-картой;
- блокировка карты после нескольких попыток ввести неверный PIN-код;
- защита «кодом владельца» (владелец – это юридическое лицо, которое вводит карты в обращение, обслуживает их и, соответственно, определяет содержимое).

В этом типе карт сосуществуют две технологии: ЭППЗУ с однократной записью (OTP EPROM) – нестираемая память, поскольку кристалл помещен в непроницаемую для ультрафиолетовых

лучей оболочку, и ЭСППЗУ – стираемая, а затем перепрограммируемая. Объем свободной памяти, как правило, меньше 1 Кбит.

Первой картой в этом семействе является TELECARTE, применяемая теперь и в других областях (киноабонемент – CINECARTE; оплата муниципальных парковок – PIAF; карта для оплаты мойки автомобилей – предлагается компаниями BP и MOBIL). Перечисленные карты используются и как жетоны, содержащие заранее оплаченные «единицы услуг», которые выбрасываются (или наоборот, собираются в коллекцию) после израсходования оплаченной суммы. Обладая хорошей защитой от взлома, карты подобного рода вместе с тем очень просты в применении и легко перепрограммируются.

Более совершенные карты могут найти применение в некоторых областях, требующих одновременно и лучшей защиты, и более частого обновления информации (например, простое электронное портмоне, карты контроля за доступом, портативные защищенные досье, абонементные карты, удостоверения и т.д.).

КАРТЫ С МИКРОПРОЦЕССОРОМ

Карты с микропроцессором (другими словами, с микро-ЭВМ) представляют собой наивысшее достижение в области развития чип-карт: это настоящая микро-ЭВМ, которая содержит ЦПУ, память программ и память данных, распределенных и организованных особым образом. Программное обеспечение в полном объеме позволяет поддерживать множество систем защиты, а именно:

- область памяти, защищенную от записи – или одновременно от записи и чтения – секретным «кодом владельца» при продаже (персонализации) карты;
- область памяти, защищенную от записи и считывания секретным «кодом пользователя» (PIN-кодом);
- блокировку карты после нескольких подряд попыток ввести неверный PIN-код, с возможностью разблокирования «владельцем»;
- использование алгоритмов шифрования (например, DES и RSA) для обеспечения безопасности обмена данными.

Существуют карты с микропроцессором, предназначенные для использования только в какой-либо одной области, и многофункциональные карты, позволяющие совмещать абсолютно автономные сферы применения. Большинство карт с микропроцессором поддерживается мощной операционной системой, именуемой, например,

COS (Chip Operating System или Card Operating System – чиповая или карточная операционная система) по аналогии с DOS (Disk Operating System – дисковая операционная система) для ПК. Речь в данном случае идет о записанном в масочное ПЗУ программном обеспечении, которое обеспечивает:

- разбиение всего свободного пространства памяти на простейшие зоны, защищаемые или не защищаемые;
- динамическое распределение памяти;
- управление конфиденциальными кодами;
- загрузку во время персонализации специальных подпрограмм, необходимых при данном применении.

Пользователь может оставлять COS такой, какая она есть, либо дополнять ее своими подпрограммами, расположенными в ЭППЗУ или ЭСППЗУ; также можно придумать свою маску для ПЗУ, частично или полностью заменяющую COS. Карты с микропроцессором подходят для самых экономически уязвимых сфер (банковские, медицинские карточки, ТВ-карты и т.д.).

ДРУГИЕ УСТРОЙСТВА, ИСПОЛЬЗУЮЩИЕ ПАМЯТЬ

Наряду с семейством классических карт, которые мы только что описали, было создано несколько оригинальных технологий. Несомненно, они также заслуживают внимания.

Хотя микросхемы памяти и микропроцессоры специально задумывались для использования совместно с микромодулями, однако в действительности микросхемы могут быть размещены на других носителях. В качестве примера можно привести ключ из пластика и соответствующий ему «замок», оснащенный специальным соединителем (подобные системы предлагают, в частности, SEFEA и Gemplus), а также «ключ», который используется в некоторых телевизионных декодерах с платным доступом к каналам. Кроме оригинального внешнего вида, преимущество заключается в значительно более высокой надежности ключа по сравнению с картой.

Проблемы авторских прав и патентов на подобные изделия, вероятно, решаются совершенно особым образом, поскольку карточки как таковой в прямом смысле этого слова нет.

КАРТЫ И БЕСКОНТАКТНЫЕ УСТРОЙСТВА

Использование контактов в традиционной электронной карточке создает проблемы при ее использовании, а иногда даже является

неизбежным недостатком во многих потенциальных областях применения чип-карт. Работа электронных карт, описанных выше, полностью зависит от качества и надежности контактов, необходимых для подачи питания и обмена данными.

Данный принцип устройства порождает не только проблемы надежности (загрязнение, износ контактов, уязвимость считывающих устройств), но и закрывает доступ к многочисленным областям применения чип-карт.

Безусловно, владельцу банковской или иной платежной карты покажется по меньшей мере странным, если появится возможность дебитировать его карту на расстоянии, причем без его подтверждения (без своеобразной «росписи»). Но во многих других областях бесконтактные карты представляют практически неограниченные возможности и удобства в обращении.

Если устранить использование контактов, электронная карточка может стать чрезвычайно надежной и, таким образом, сможет переносить воздействие самых тяжелых условий и агрессивных сред: непогоду, морской соляной туман, высокие температуры, химически активные вещества... Это особенно удобно в промышленности и при использовании на открытом воздухе (например, в автомобильном сервисе, на морском транспорте или в спорте).

Возможность бесконтактной связи, причем на некотором расстоянии, позволяет осуществлять обмен информацией даже «в движении», например в случае идентификации лиц, проходящих через открытую дверь; распознавания транспортных средств, без остановки пересекающих пост сбора дорожной пошлины; учета деталей на поточной линии или конвейере; нанесения неудаляемой маркировки на арендуемое оборудование или даже клеймения электронным тавро крупного рогатого скота или иных животных, и т.д.

Устройства, известные под названием «транспондер», наделенные подобными функциями, существуют уже с давних пор и иногда используются в промышленности и транспорте. Речь идет о дорогостоящем и относительно громоздком оборудовании, которое не может быть размещено на пластиковой карте стандартного размера, главным образом из-за малой толщины карты.

Постоянная миниатюризация компонентов и уменьшение потребляемой ими мощности позволяют теперь рассматривать возможность создания устройств, которые снабжены энергонезависимой памятью и способны обмениваться данными со специальным блоком чтения-записи, расположенным на расстоянии от нескольких

сантиметров до одного метра. Такое устройство могло бы питать микросхему на расстоянии посредством магнитной индукции. Отсутствие элемента питания в устройстве является определяющим фактором в плане удобства и компактности.

Но практическая реализация таких идей остается весьма сложной, несмотря на простоту этого принципа. Необходимо использовать сложные виды модуляции и системы синхронизации, чтобы гарантировать очень высокую степень надежности работы всей системы в рассматриваемых областях. Появление электронных компонентов, специально разрабатываемых для подобных целей, позволяет надеяться, что в недалеком будущем бесконтактные чип-карты прочно войдут в обиход.

ТИПОРАЗМЕРЫ

Известно, что обычные чип-карты имеют те же размеры, что и карты с магнитными дорожками, а именно около 85×54 мм, толщина 0,76 мм. Однако современные блоки чтения-записи получаются слишком громоздкими и не могут быть встроены в некоторые виды оборудования. Поэтому были созданы миниатюрные карты – основной целью их разработки была минимизация пустой площади вокруг микромодуля. Так появились очень маленькие электронные карты, размером с почтовую марку, называемые SIMCARD и используемые главным образом в портативных телефонах стандарта GSM.

РАЗМЕЩЕНИЕ И ОБОЗНАЧЕНИЕ КОНТАКТОВ

Разумеется, были разработаны правила, призванные по возможности стандартизовать контактные пары электронных карт и картоприемников. Самые старые чип-карты (телефонные, банковские и т.п.) выполнялись по стандарту AFNOR, поскольку были изобретены во Франции. Этот стандарт называют также «смещенные контакты»; пример показан на рис. 1.1.

Затем появились международные стандарты ISO 7816, определяющие центральное расположение контактов микромодуля с дополнительным разворотом его на 180°. Из рис. 1.2 видно, почему такое расположение контактов получает все большее распространение. Предполагается постепенно перейти к такой конфигурации всех типов карт, даже если это и потребует модернизации существующего оборудования.

Топология «Международной Организации по Стандартизации» (ISO) выделяет для микромодуля место между зоной, отведенной

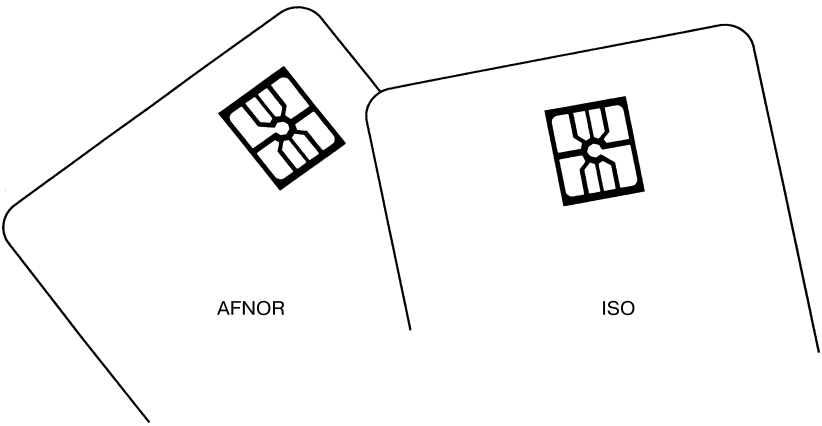

Рис. 1.1. Два стандарта расположения кристалла микросхемы

на обороте магнитным полоскам, и зоной на лицевой стороне, предназначенной для размещения текста, выполняемого тиснением, который при совершении сделок может быть скопирован продавцом на квитанцию (слип) при помощи специального устройства.

Рис. 1.2. Назначение различных зон карты

На самом деле иногда возможно разместить микромодуль и магнитные дорожки в одной и той же зоне, как это было сделано, например, на кредитных карточках VISA. Но при этом пользоваться ими приходилось очень аккуратно – рекомендация ISO не давала

никакого преимущества, так как микромодуль, размещенный по центру, все равно попадал в зону неиспользуемой теперь дорожки T2, как показано на рис. 1.3.

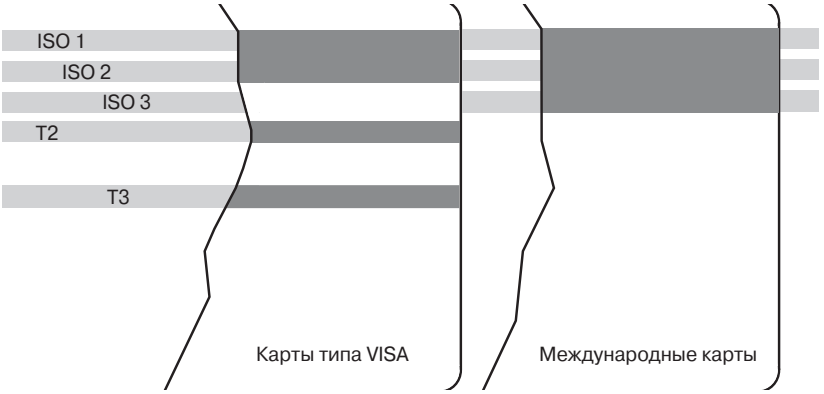

Рис. 1.3. Стандартное расположение магнитных полос

Таким образом, стандарт определяет и нумерацию контактов микромодулей, которые могут включать в себя до восьми контактов, расположенных согласно рис. 1.4. Из них два контакта зарезервированы для возможного использования в будущем и обозначаются RFU. Нередко встречаются микромодули только с шестью контактами.

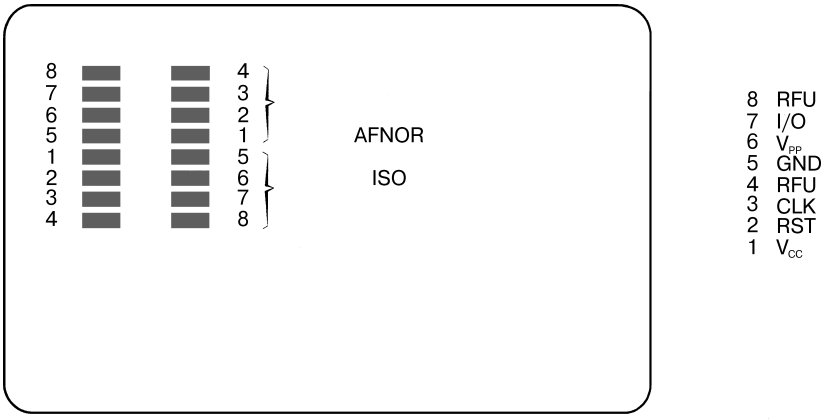

Рис. 1.4. Нумерация контактов микромодулей