Mifare — стандарт № 1 в бесконтактной идентификации

Ирина СОКОЛОВА
sokolova.i@mtgroup.ru

В данной статье пойдет речь о стандарте NXP Mifare 13,56 МГц, соответствующем стандартам радиочастотной идентификации ISO 14443 A, ISO 14443 B и ISO 15693. Стандарт Mifare обеспечивает дальность считывания в пределах нескольких сантиметров. Данная технология принадлежит компании NXP Semiconductors.

В настоящее время технологии контактной и бесконтактной идентификации получают колоссальное распространение в России и мире. Количество сфер применения данных технологий постоянно растет. Вот далеко не полный список тех отраслей, где применяется RFID:

- электронные системы контроля доступа в здание;
- системы идентификации водителя в автомобиле;
- транспортная и складская логистика;
- медицина — мониторинг состояния пациентов;
- библиотеки — станции автоматической книговыдачи, быстрая инвентаризация;
- электронные паспорта;
- транспортные и другие платежи;
- дистанционное управление;
- идентификация животных.

Для различных применений существуют различные стандарты RFID.

С начала 1990-х годов было изобретено множество протоколов радиочастотной идентификации. Чтобы их упорядочить, была создана организация — разработчик стандартов RFID: EPCglobal, а впоследствии еще одна организация — AIM global. В конце 2007 года автомобильный концерн Daimler AG присоединился к EPCglobal group. Данные организации не занимаются выпуском RFID-продуктов, они только разрабатывают стандарты.

Существует ряд компаний, которые зарекомендовали себя в качестве крупнейших производителей микросхем для RFID-меток и считывателей, среди них NXP Semiconductors, Infineon, Texas Instruments.

Безусловным лидером производства микросхем для бесконтактных микросхем и RFID является NXP Semiconductors: 80% электронных паспортов и более 80% электронных проездных билетов в общественном транспорте во всем мире основаны на микросхемах NXP.

Компания NXP выпускает микрокомпоненты для построения систем радиочастотной идентификации на базе стандарта Mifare и других стандартов, которые входят в портфель интеллектуальной собственности NXP (наряду с Hitag, UCODE, ICODE и др.).

Любая система идентификации обычно состоит из считывателя (ридера) и метки (транспондера). В зависимости от дальности считывания метка может быть активной или пассивной (соответственно с наличием или отсутствием собственного источника питания).

Активные метки используются в тех системах, где необходимо обеспечить большое расстояние считывания. Метка в этом случае — излучателем достаточно мощного сигнала, источником энергии для которого является собственный источник питания. Пассивные метки используются для недорогих систем. Пассивная метка не излучает сигнал, а только модулирует энергию электромагнитного поля, излучаемого ридером, и поэтому не нуждается в собственном источнике питания. А ридер в этом случае фиксирует модуляцию излучаемого им электромагнитного поля, осуществляемую меткой.

Платформа Mifare представлена набором считывателей и микросхемами для смарт-карт, которые могут поддерживать различные стандарты криптозащиты, размеры памяти, количество циклов перезаписи и т. д.

В принципе, компания NXP позиционирует Mifare даже не как RFID (поскольку чистая радиочастотная идентификация представлена в портфолио NXP такими стандартами, как ICODE, Hitag, UCODE), а как интерфейсную платформу для бесконтактных смарт-карт (рис. 1). Действительно, несмотря на сравнительно небольшое расстояние считывания (до 10 см), Mifare обладает множеством характеристик, необходимых для различных сложных применений, например, криптозащита, наличие EEPROM, а новейшие микросхемы меток семейства Mifare можно также программировать, поскольку в них используются микроконтроллеры.

Что касается меток Mifare, то для них стандарт представлен следующими подсемействами:

- Mifare Ultralight;
- Mifare Classic (Standard) Mini/1/4 кбайт;
- Mifare Plus (выпуск ожидается в 3-м квартале текущего года).
- Mifare DesFire8 2/4/8 кбайт.
- SmartMX с объемом памяти EEPROM от 5 до 144 кбайт и возможностью эмуляции карт Mifare 1/4 кбайт.

Рис. 1. Ридер Pegoda

Рассмотрим характеристики данных подсемейств, возможности их применения и продукты, предлагаемые в каждом из подсемейств компанией NXP.

Mifare Ultralight

Mifare Ultralight (рис. 2) был разработан специально с учетом нужд оплаты проезда в общественном транспорте, совместно с провайдерами услуг, системными интеграторами и производителями бумаги для смарт-карт.

Поэтому он идеально подходит для бюджетных систем с большим количеством пользователей, например, для оплаты проезда в общественном транспорте, для систем продажи билетов на различные мероприятия и для многих других применений.

Преимущества:

- EEPROM 512 бит с возможностью перезаписи;
- совместим с существующей инфраструктурой Mifare;
- расстояние считывания до 10 см;
- система антиколлизии;
- используется с пассивными метками;
- возможна организация полностью бесконтактной системы;
- сокращение механических повреждений систем контроля доступа;
- сокращение затрат на установку системы и затрат на ремонт и обслуживание;
- наиболее усовершенствованная статистическая система сбора данных.

Возможность перезаписи позволяет использовать карту многократно. Mifare Ultralight позволяет создавать бесконтактные системы контроля доступа с расстоянием считывания до 10 см. При этом, благодаря системе антиколлизии, через один пункт контроля доступа может проходить одновременно несколько пользователей. В Mifare Ultralight используется пассивная метка, не требующая дополнительного питания. Такая метка может быть размещена на плоском бумажном или пластиковом носителе, что позволяет снизить стоимость смарт-карты для конечного пользователя и использовать ее многократно.

Mifare Standard (Classic)

Это подсемейство представлено микросхемами меток Mini/1K/4K EEPROM (S20, S50, S70).

Mifare Classic — это пионер и лидер в технологии бесконтактных смарт-карт с возможностью перезаписи, работающих в диапазоне частот 13,56 МГц. Впервые тонкая ISO-карта с антенной по стандарту Mifare была выпущена в 1995 году.

Стандарт Mifare был впервые использован для продажи билетов в общественном транспорте в столице Кореи, Сеуле. После этого стандарт также был использован для продажи билетов в общественном транспорте таких крупных городов, как Лондон, Пекин, Тайбэй и многих других. В России данный стандарт также используется в системах оплаты метрополитенов Санкт-Петербурга и Москвы.

Рис. 2. Карты Mifare: Mifare Ultralight, Mifare Standart 1K, Mifare Standart 4K

С появлением контроллера дуального интерфейса Mifare начали использовать в закрытых билетных системах, где происходит безопасная авторизованная оплата. Дуальный интерфейс позволяет использовать микросхемы меток Mifare как в контактных, так и в бесконтактных системах. Этот стандарт также широко применяется для билетов с фиксированной стоимостью, например для проездных билетов на неделю или на месяц.

Продукты Mifare Classic могут использоваться для платежей в других системах, например как пропуск на платные парковки (с возможностью отследить время прибытия и выезда с платной стоянки). Такие авиакомпании, как Lufthansa и Air France, применяют технологию Mifare для карт постоянных клиентов, компания Shell основала на стандарте Mifare систему платежей за бензин Shell Easypay.

Mifare Classic и Mifare Ultralight являются универсальными стандартами, и единственный их недостаток, из-за которого они не могут быть использованы в системах контроля доступа, заключается в том, что в них реализован простейший алгоритм криптозащиты CRYPTO-1. В других подсемействах Mifare реализованы более сложные аппаратные алгоритмы криптозащиты: AES, DES и PKI.

В марте 2008 года в мировых и российских специализированных СМИ активно обсуждался взлом хакерами алгоритма CRYPTO-1 (в частности, информацию об этом можно посмотреть на сайте **www.computerra.ru**). Компания NXP опубликовала официальный ответ на обсуждение взлома этого крипто-алгоритма на сайте **www.mifare.net**.

Mifare DesFire8

Mifare DesFire8 — это первая бесконтактная система на рынке, которая поддерживает Усовершенствованный Стандарт Кодирования — Advanced Encryption Standard (AES) а также общие криптографические методы, такие как DES и 3DES.

Преимущества:

- полностью совместим со стандартом ISO 14443A 1-4;
- программируемая EEPROM 2/4/8K;
- безопасный высокоскоростной набор команд;
- гибкая файловая структура;
- система антиколлизии;
- уникальный 7-байтный серийный номер (по системе ISO уровень 2);
- аппаратно реализованный открытый криптоалгоритм DES/3DES;
- аппаратно реализованный открытый криптоалгоритм AES128.

По этому стандарту выполнены микросхемы меток с EEPROM 2/4/8K (D21, D40, D41, D81). Mifare DesFire8 может применяться в системах, где необходима высокоскоростная передача данных с повышенной безопасностью. Продукты Mifare DesFire8 обладают гибкой организацией памяти и могут взаимодействовать с существующей инфраструктурой Mifare. Mifare DesFire8 совместим со всеми 4 уровнями стандарта ISO / IEC 14443A и использует дополнительные команды стандарта ISO / IEC 7816-4.

Карта, основанная на Mifare DesFire8, может использоваться в 28 различных системах и иметь в памяти до 32 файлов на каждую систему. Размер каждого файла определяется в момент его создания, что делает Mifare DesFire8 гибким и удобным продуктом.

Mifare DesFire8 имеет высокий уровень безопасности благодаря аппаратному криптогра-

фическому инструменту 3DES, используемому для зашифровки передаваемых данных.

Mifare DesFire8 обеспечивает множество преимуществ конечным пользователям, позволяя записывать на карту бесконтактные билеты, использовать карту для платежей в торговых автоматах, а также для доступа, например, в офис.

SmartMX

Smart MX — это семейство микроконтроллерных карт с поддержкой нескольких интерфейсов (контактного, бесконтактного и USB). Уровень криптозащиты SmartMX еще выше, чем у DesFire8: это семейство отвечает стандартам криптозащиты 3DES, AES и PKI (Public Key Infrastructure). Размер памяти данного продукта может быть гораздо больше, чем у других подсемейств Mifare (от 5 до 144 кбайт).

Smart MX могут эмулировать карты Mifare 1 кбайт и Mifare 4 кбайт (рис. 2). Помимо бесконтактного, SmartMX могут работать с контактным интерфейсом стандарта ISO 7816 и USB 2.0.

Карты на базе чипов семейства SmartMX могут применяться в четырех основных областях, требующих защиты информации: электронные документы, платежные и банковские карты, транспортные карты, мобильные приложения.

При этом семейство SmartMX может взаимодействовать с существующей инфраструктурой Mifare — никаких обновлений системы не требуется.

Mifare Plus

10 марта 2008 года компания NXP объявила о том, что в четвертом квартале 2008 года будет выпущена микросхема транспондера нового стандарта Mifare Plus . Являясь модификацией стандарта Mifare Classic, Mifare Plus позволяет реализовать защиту информации для применений низкого ценового диапазона, в особенности для реализации систем оплаты проезда в городском транспорте при помощи бесконтактных смарт-карт, а также для применений в системах контроля доступа.

Mifare Plus — это последнее добавление NXP к портфолио Mifare, которое имеет несколько уровней криптозащиты, включая AES, а также обладает всеми свойствами стандарта Mifare Classic.

С Mifare Plus пользователи могут быть уверены, что их персональная информация не будет отслежена другими. Mifare Plus предоставляет высокую гибкость, поддерживая несколько уровней безопасности и обеспечивая простое усовершенствование существующей системы, реализованной на Mifare Classic, и обладает при этом приемлемой стоимостью.

Семейства считывателей Micore и Micore 2

Для организации систем идентификации Mifare компания NXP предлагает два семейства считывателей — Micore и Micore 2.

Семейство считывателей Micore представлено четырьмя продуктами:

- MFRC500;
- MFRC530;
- MFRC531;
- CLRC 632.

Все микросхемы повыводно совместимы между собой. Для того чтобы заменить одну микросхему на другую в системе, разработчику не нужно менять программное обеспечение.

Семейство считывателей Micore 2 представлено двумя продуктами:

- MFRC522;
- MFRC523.

Micore 2 оптимизировано для портативных считывателей (сниженное энергопотребление, уменьшенные корпуса микросхем). MFRC522 и MFRC523 выпускаются в корпусе HVQFN32 и являются повыводно совместимыми между собой. Они обладают интерфейсами RS-232, SPI и I^2C.

Отладочные средства

В качестве отладочных средств для стандарта Mifare компания NXP предлагает готовые комплекты MFEV700, MFEV800 и CLRD701 на базе считывателей Pegoda с образцами карт. Также на сайте NXP в свободном доступе есть программное обеспечение для работы с ридерами.

Таким образом, на сегодняшний день компания NXP предлагает полный набор компонентов, необходимый для разработки систем бесконтактной идентификации для различных применений.