

Продукция компании Infineon Technologies для приложений идентификации

Количество технологий электронной идентификации так же велико, как и число возможных их применений. Среди весьма широкого перечня производителей компонентов для задач идентификации компания Infineon Technologies занимает ведущие позиции как в широком секторе полупроводниковых компонентов для интеллектуальных карт (Smart Cards), так и в сегменте рынка полупроводниковых компонентов для идентификации. Стремительно развивающийся сегмент рынка приложений идентификации на базе интеллектуальных карт и электронных меток обостряет конкуренцию среди поставщиков компонентов и решений для задач электронной идентификации. Занимая существенную долю рынка компонентов и средств для электронной идентификации, Infineon Technologies располагает сегодня широким ассортиментом чипов и обеспечивает заказчиков поддержкой на всех стадиях проекта разработки.

Сергей Гуцин

vv-intec@aha.ru

Обеспечение высокого уровня безопасности и надежности сохранения данных является приоритетной задачей разработчиков компонентов для идентификации компании Infineon Technologies. Каждый выпускаемый прибор, будь то бесконтактная метка или 32-разрядный контроллер, подлежит обязательной сертификации на соответствие тем или иным приложениям или условиям применения (<http://www.silicon-trust.com/index.asp>).

Весь спектр выпускаемых полупроводниковых компонентов для приложений идентификации по типу интерфейса с терминалом можно разделить на бесконтактные и контактные, а по внутренней

структуре — на элементы на основе памяти (memory-based) и на основе контроллера (controller-based).

Для приложений идентификации на базе контактных терминалов компанией Infineon Technologies предлагается наиболее широкий перечень компонентов, из которого в подавляющем большинстве случаев можно выбрать оптимальное решение при доступной стоимости и традиционно высоком уровне безопасности. В таблице 2 представлена номенклатура и основные характеристики кристаллов с контактным интерфейсом на основе памяти. Основными областями применения данных продуктов можно назвать приложения для медицины, платные теле-

Таблица 1. Десять наиболее популярных кристаллов производства Infineon для приложений идентификации

Обозначение	SLE 4428	SLE 44R35	SLE 55R16	SLE 66CL81P	SLE 66CLX320P	SLE 66CX162PE	SLE 66CX322P	SLE 66CX642P	SLE 88CX720P	SLE 88CFX4000P
Описание кристалла	Защищенная память	Защищенная память с бесконтактным интерфейсом	Контроллер с бесконтактным интерфейсом	Криптографический контроллер с комбинированным интерфейсом	Криптографический контроллер					
Приложения	Идентификация	Идентификация/транспорт	Идентификация/транспорт	Идентификация/транспорт	Идентификация с высоким уровнем защиты и безопасности. Многозадачность.	Идентификация с высоким уровнем защиты и безопасности. Многозадачность.	Идентификация с высоким уровнем защиты и безопасности. Многозадачность.	Идентификация с высоким уровнем защиты и безопасности. Многозадачность.	Идентификация с высоким уровнем защиты и безопасности. Многозадачность.	Идентификация с высоким уровнем защиты и безопасности. Многозадачность.
Размер EEPROM	1 кбайт	1 кбайт	2,56 кбайт	8 кбайт	32 кбайт	16 кбайт	16 кбайт	64 кбайт	72 кбайт	400 кбайт

Таблица 2. Основные характеристики кристаллов с контактным интерфейсом на основе памяти

Обозначение	SLE4428	SLE 4418	SLE 4442	SLE 4432	SLE 6636	SLE 7736
Описание кристалла	Защищенная память				Защищенная память со счетчиком в EEPROM	
Приложения и особенности	Идентификация/хранение данных с шифрованием информации и блокировкой записи	Идентификация/хранение данных с блокировкой записи	Идентификация/хранение данных с шифрованием информации и блокировкой записи	Идентификация/хранение данных с блокировкой записи	Идентификация данных с высоким уровнем безопасности и защиты. Специализированная технология IMEM. Функция периодической повторной аутентификации. Два ключа доступа.	Идентификация данных с высоким уровнем безопасности и защиты. Функция периодической повторной аутентификации. Два ключа доступа. Механизм принудительного физического разрушения карты
Размер EEPROM	1 кбайт	1 кбайт	256 байт	256 байт	237 бит	237 бит

Таблица 3. Характеристики некоторых кристаллов производства Infineon с бесконтактным интерфейсом на основе памяти

Обозначение	55R01	55R16	55V02P	55V10S	44R35S	66R35
Тип кристалла	my-d Proximity		my-d Vicinity		Mifare	
Стандарт интерфейса	ISO/IEC 14443 (Тип A)	ISO/IEC 14443 (Тип A)	ISO/IEC 15693	ISO/IEC 15693	ISO/IEC 14443 (Тип A)	ISO/IEC 14443 (Тип A)
Приложения и особенности	Гибкая структура памяти (до 14 секторов). Защита передаваемых данных. Контроль доступа	Гибкая структура памяти (до 14 секторов). Защита передаваемых данных. Контроль доступа	Незащищенная память с бесконтактным интерфейсом. Идентификация почтовых отправлений, грузов, автоматизация производственных и складских операций	Гибкая структура памяти (до 16 секторов). Защита передаваемых данных. Идентификация товаров, отправлений, грузов, автоматизация платежей и хранение данных. Контроль доступа	Полностью сертифицирован на соответствие стандарту Mifare. Уникальный серийный номер. Трехуровневая аутентификация на базе ключей длиной 48 бит.	Полностью сертифицирован на соответствие стандарту Mifare. Уникальный серийный номер. Трехуровневая аутентификация на базе ключей длиной 48 бит
Размер EEPROM пользователя	128 байт	2048 байт	2048 бит	8192 бит	768 байт	768 байт
Размер EEPROM администратора	32 байт	512 байт	512 бит	2048 бит	256 байт	256 байт
Рабочее расстояние	0–10 см	0–10 см	0–70 см в зависимости от конфигурации антенны	0–70 см в зависимости от конфигурации антенны	0–10 см	0–10 см и более в зависимости от конфигурации антенны

Таблица 4. Основные характеристики кристаллов с контактным интерфейсом на основе контроллера

Семейство контроллеров	SLE66P		SLE66PE		SLE88	
Обозначение	66C322P	66CX642P	66CX162PE	66CX680PE	SLE 88CX720P	SLE 88CFX4000P
Размер ROM	134 кбайт	206 кбайт	96 кбайт	246 кбайт	240 кбайт	80 кбайт
Размер EEPROM	32 кбайт	64 кбайт	16 кбайт	68 кбайт	80 кбайт	400 кбайт
Размер RAM	4352 байт	4352 байт + 700 байт	5 кбайт	7100 байт	8 кбайт + 700 байт	16 кбайт + 800 байт
Тактовая частота	1–10 МГц	1–15 МГц	1–33 МГц	1–33 МГц	до 66 МГц	до 66 МГц
Периферийные модули	UART, PLL, CRC, 2 таймера 16 разрядов	UART, PLL, CRC, 2 таймера 16 разрядов	UART, RNG, DES, ACE, 2 таймера 16 разрядов	UART, RNG, DES, ACE, 2 таймера 16 разрядов, SEMA/DEMA, SPA/DPA, DFA, chip ID	UART, RNG, DES, ACE, 2 таймера 16 разрядов, SEMA/DEMA, SPA/DPA, DFA, 3DES in HW, chip ID	UART, RNG, DES, ACE, 2 таймера 16 разрядов, SEMA/DEMA, SPA/DPA, DFA, 3DES in HW, chip ID
Приложения и особенности	Идентификация товаров и объектов, контроль доступа и учет	Идентификация, платные телекоммуникационные услуги, контроль доступа и учет	Идентификация, платные телекоммуникационные услуги, контроль доступа и учет	Идентификация, платные телекоммуникационные услуги, контроль доступа и учет	Идентификация и хранение защищенных данных, контроль доступа и учет, Java, цифровая подпись	Идентификация и хранение защищенных данных, контроль доступа и учет, Java, цифровая подпись
Напряжение питания	2,7–5,5 В	1,62–5,5 В	2,7–5,5 В	1,8; 3,0; 5,0 В	2,7–5,5 В	1,62–5,5 В

коммуникационные услуги и локальные платежные системы. Выпуск наиболее распространенного на сегодняшний день кристалла SLE4436 (Eurochip 1) прекращен в 2002 году, завершение производства его расширенной версии планируется в конце 2004 года. На смену им приходят кристаллы с улучшенными характеристиками, изготовленные на базе более «тонких» полупроводниковых технологий, что позволит компании Infineon Technologies предлагать их в будущем по более низкой цене.

Для новых проектов и перспективных разработок целесообразно использовать кристаллы SLE6636 (Eurochip 66) и SLE7736 (Eurochip 77). Поддерживая совместимость снизу вверх, микросхема SLE7736 обладает рядом дополнительных функций, которые делают ее наиболее защищенной на сегодняшний день. Специализированная патентованная технология IMEM, применяемая при производстве SLE7736, призвана усложнить чтение защищенных данных путем физического воздействия на кристалл. Интересной новой функцией является механизм принудительного физического разрушения карты (CTM — Card Trash Mechanism), который активизируется при достижении счетчиком в EEPROM нулевого значения. Для предотвращения доступа к данным посредством изменения электрических параметров в кристалл интегрированы соответствующие датчики, при срабатывании любого из которых доступ к данным блокируется. Поставка производителем микросхем SLE7736 осуществляется в комплекте с модулем M3.2 с возможностью за-

несения данных на этапе производства и защитой транспортным кодом.

Весь спектр производимых кристаллов для бесконтактной идентификации на базе памяти можно условно разделить на следующие типы: my-d proximity, my-d vicinity, Mifare. Ключевыми параметрами при выборе нужного решения являются максимальное расстояние между меткой на основе кристалла и терминалом, величина и организация EEPROM, система защиты считываемых данных, стоимость и физические размеры кристалла идентификационной метки. В таблице 3 приведены характеристики некоторых кристаллов с бесконтактным интерфейсом на основе памяти производства Infineon. Полный перечень выпускаемых в настоящее время кристаллов доступен в Интернете по адресу http://www.infineon.com/cgi/ecrm.dll/ecrm/scripts/prod_cat.jsp?oid=8232.

Для поддержки разработки новых систем на базе кристаллов для бесконтактной идентификации доступны два стартовых комплекта: CR-EVA-kit для Proximity и Mifare (http://www.infineon.com/cgi/ecrm.dll/ecrm/scripts/prod_ov.jsp?oid=14537&cat_oid=-9355), а также my-d vicinity kit для микросхем Vicinity (http://www.infineon.com/cgi/ecrm.dll/ecrm/scripts/prod_ov.jsp?oid=29315&cat_oid=-9355). В зависимости от требований заказчика возможны три варианта поставки: кристаллы на пластине, на основе модулей MCC2 или MCC, на ленте с размерами 76×45 мм или 45×45 мм.

С целью облегчения построения терминального оборудования и различных считывателей данных Infineon предлагает ряд спе-

циализированных микросхем. Для построения бесконтактного интерфейса в соответствии со стандартом ISO 14443 предназначена микросхема SLEF9000N. Ею поддерживаются оба используемые типа модуляции (A и B), а также функция разрешения коллизий с мультиплексируемым параллельным интерфейсом для связи с управляющим процессором. Для построения модуля безопасности, иначе называемого SAM-модулем, можно применить микросхему SLEF9611 (http://www.infineon.com/cgi/ecrm.dll/ecrm/scripts/prod_cat.jsp?oid=9356), работающую с кристаллами и метками Infineon типа 55Rxx.

Начало выпуска микросхем для задач идентификации на основе контроллера датируется 1993 годом, когда появился 8-разрядный кристалл серии 44S (в то время выпускался компанией Siemens). С 1998 года основным продуктом стало семейство 16-разрядных микросхем 66P, которое, в свою очередь, постепенно вытесняется выпущенной в 2000 году серией 66S на основе технологии 0,25 мкм. Рекомендуемым для новых разработок можно назвать наиболее популярное на сегодняшний день семейство 66PEhanced, которое появилось несколько позднее и, как видно из обозначения, является улучшенной версией предыдущего семейства. В таблице 4 приведены характеристики некоторых кристаллов с контактным интерфейсом на основе контроллера. Ключевыми областями применения данных микросхем были и остаются приложения, где необходима защита больших объемов данных и поддержка нескольких приложений на одном кристалле (многозадачность), причем наравне с приложениями идентификации зачастую могут выпол-

няться иные задачи. В 2002 году завершена квалификация кристалла 88CX720P (0,22 мкм) — первого 32-разрядного контроллера, за которым последовал выпуск 88CFX4000P (0,13 мкм). Данные приборы ориентированы на многозадачные приложения, включающие различные функции идентификации при аппаратной поддержке криптографических алгоритмов 3DES, AES, RSA и ряда других.

Кристаллы на основе контроллера с комбинированным интерфейсом (стандартный + бесконтактный) производства Infineon изготавливаются в соответствии со спецификацией ISO 14443 при рабочей частоте 13,56 МГц

(методы модуляции А и В). На сегодняшний день наиболее популярными продуктами данной серии являются микросхемы SLE66CL81P, SLE66CL160S, SLE66CLX320S. Наравне с поддержкой всех функций соответствующих семейств контроллеров, данные приборы снабжены специальными средствами управления потоком передачи данных по радиоканалу, что позволяет оптимизировать энергопотребление и увеличить плотность передачи данных.

Для самостоятельной разработки заказчиком собственного ПО компанией Infineon Technologies предоставляются различные

программные средства, включающие как готовые операционные системы, так и библиотеки функций. Доступные средства разработки включают весь спектр необходимого оборудования и программных средств для проведения всего цикла разработки программного обеспечения вплоть до выпуска тестовой партии пластиковых карт на основе продукта SmartMask. В качестве средств разработки программного обеспечения можно использовать программный симулятор, поставляемый в составе SDK CC, полный аппаратный эмулятор Hitex ET66P, а также монитор ПЗУ RM66P и различные эмуляторы карт. ■