Патрик Гёлль

ПК и чип-карты

Patrick Gueulle
Ingénieur EFREI

PC et CARTES À PUCE





EDITIONS TECHNIQUES ET SCIENTIFIQUES FRANÇAISES

В помощь радиолюбителю

Патрик Гёлль

Инженер EFREI

ПК и ЧИП-КАРТЫ

ДМК ПРЕСС
издательство

СОДЕРЖАНИЕ

Предисловие 8

1 Микропроцессоры чип-карт 9
- Микропроцессоры, микрокалькуляторы или микроконтроллеры? 10
- Материальные ресурсы 10
- Программные ресурсы 14
- Ресурсы, обеспечивающие безопасность 17
- Несколько понятий из криптографии 19
- Понятие маски 23
- Маски BULL CP8 23
- Маски COS 30

2 Исследования банковской карты 35
- Вариант маски BULL CP8 M4 36
- Устройство чтения-записи для карт на микропроцессоре 37
- Правильное использование конфиденциального кода 43
- Контроль расходов 47
- Набор рабочих инструментов для банковской карты 47
- Как читать магнитные полосы 54
- Перспективы 56

3 Мини-система разработки 67
- Адаптер RS232 для асинхронных карт 68
- Малогабаритный анализатор протокола 71
- Малогабаритный имитатор карт 75
- Экспериментальная чип-карта на PIC16CXX 81

Телефонные, или синхронные, карты 101
Мини-устройство чтения-записи ISO/AFNOR 102
Распознавание чипов
с помощью специальной программы
111
Телефонные карты и защита программного обеспечения
114
T2G, телефонная карта второго поколения 117
Европейские карты 126

Программы и файлы 133
Особенности программ 134
Инсталляция программ 140
Способ использования программы CARTES.EXE 141

ПРЕДИСЛОВИЕ

Когда в 1992 году была выпущена в свет книга “Cartes à puce, Initiation et applications”[1], вряд ли кто-либо предполагал, что спустя три года невинные опыты в области чтения и записи пустых телефонных карт приведут к проникновению в секреты настоящих «электронных крепостей», каковыми могут считаться карты на микропроцессорах и новые телефонные карты с памятью, данные в которых можно обновлять.

Изготовители и дистрибьюторы самих карт, уверенные в эффективности механизмов защиты их приложений, оказали автору любезное содействие в написании данной книги, и теперь появилась возможность показать читателям, как можно преобразовать ПК в мощное орудие исследования и даже имитации самых разных чип-карт.

Несколько простейших электронных схем и специальное программное обеспечение, представленное на сервере www.dmkpress.ru издательства «ДМК Пресс», дадут вам материал для захватывающих открытий. Счастливого пути в увлекательный мир чип-карт!

[1] Русский перевод: «Чип-карты. Устройство и применение в практических конструкциях», М.: ДМК, 2000. Файлы с программным обеспечением размещены на сайте www.dmkpress.ru.

ГЛАВА СТРАНИЦА

1 МИКРОПРОЦЕССОРЫ ЧИП-КАРТ

Микропроцессоры, микрокалькуляторы или микроконтроллеры? 10
Материальные ресурсы 10
Программные ресурсы 14
Ресурсы, обеспечивающие безопасность 17
Несколько понятий из криптографии 19
Понятие маски 23
Маски BULL CP8 23
Маски COS 30

2	Исследования банковской карты	35
3	Мини-система разработки	67
4	Телефонные, или синхронные, карты	101
5	Программы и файлы	133

МИКРОПРОЦЕССОРЫ, МИКРОКАЛЬКУЛЯТОРЫ ИЛИ МИКРОКОНТРОЛЛЕРЫ?

В 1981 году, за два года до внедрения первых чип-карт, у компании BULL появились первые однокристалльные чип-карты на микрокалькуляторах.

По тем временам это было большое открытие, достигнутое благодаря сотрудничеству с компанией Motorola, поскольку с момента возникновения первых прототипов, выпущенных в 1974 году для компании Roland Moreno, имело место сочетание по крайней мере двух различных чипов (микропроцессора и памяти).

В 1976 г. компания CII Honeywell-Bull приобрела лицензию у фирмы Innovatron и приняла термин «карта на микрокалькуляторе» для обозначения продукта, который до сегодняшнего дня составляет семейство CP8. Хотя конкуренты BULL CP8 чаще употребляют сочетание «карта на микропроцессоре», в наибольшей степени соответствует истине название «карта на микроконтроллере».

На самом деле архитектура современных чипов для карт объединяет центральный процессор на 8 бит, ПЗУ, ОЗУ, ППЗУ и/или ЭСППЗУ, порты ввода-вывода точно так же, как и все микроконтроллеры. Просто в настоящее время существует тенденция добавлять все больше так называемых ресурсов для обеспечения безопасности, размещаемых на том же чипе. Таковы, вероятно, перспективы развития чип-карт.

МАТЕРИАЛЬНЫЕ РЕСУРСЫ

Если очевидным лидером на рынке инкартируемых микроконтроллеров является компания Motorola, то среди прочих производителей, по достоинству оценивших этот бизнес, наблюдается ожесточенная конкуренция. Карты начинают выпускаться в астрономических количествах!

Компания SGS-Thomson занимает особенно удачные позиции со своей продукцией, основанной на ядре, совместимом с процессорами Motorola, и очень интересными решениями в области защиты. Philips решительно выходит на сцену с архитектурой 8051, внося существенный вклад в использование возможностей криптографических вычислений. Компания Texas Instruments, прямой конкурент SGS-Thomson на рынке чипов для телефонных карт, предлагает, со своей стороны, ряд инкартируемых микропроцессоров, выросших из семейства TMS370. И конечно, данным вопросом очень пристально интересуются японские производители, в первую очередь концерн OKI с его продукцией OSCAR.

Интересно в общих чертах сравнить блок-схемы микроконтроллеров различных марок, часто встречающихся в чип-картах. На рис. 1.1 воспроизведедена общая структурная схема всех продуктов Motorola, которые имеют в своей основе классическое ядро 68HC05.

Версией SC24 (3К ПЗУ, 1К ЭСППЗУ, 128 байт ОЗУ) снабжены, в частности, французские банковские карты.

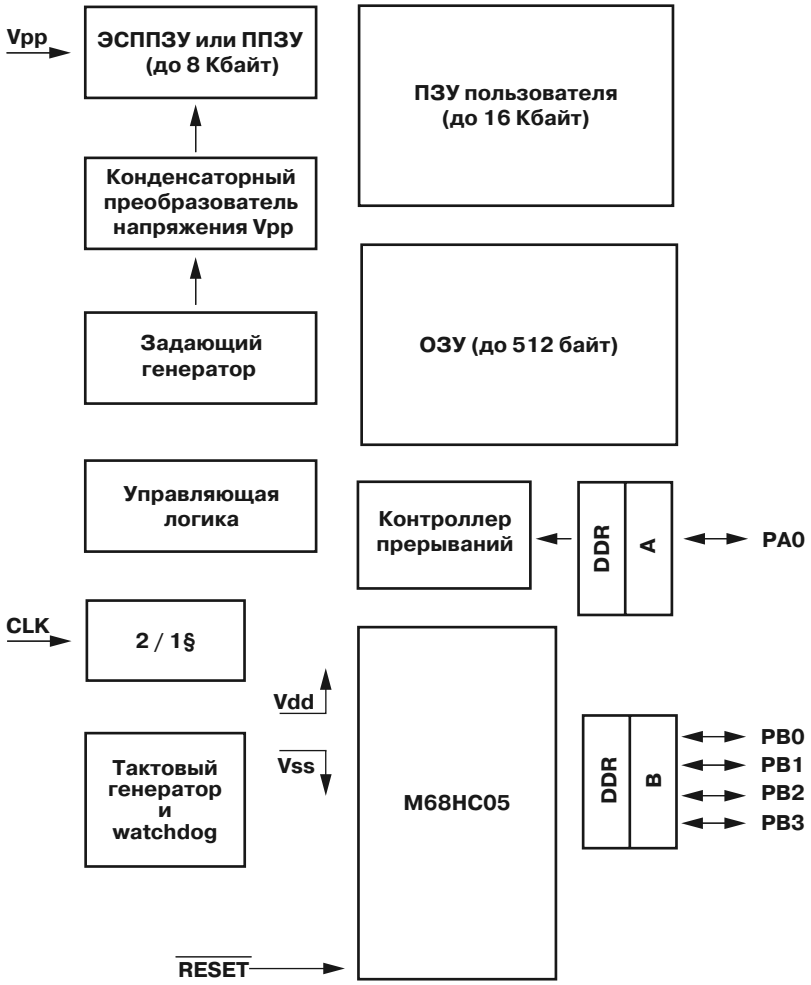


Рис. 1.1. Архитектура M68HC05SC Motorola