FUDAN MICROELECTRONICS

复旦微电子

FM11RF08

8KBits Contactless Card IC

Functional Specification

May. 2008

Content

CONTENT 3

1. FEATURES 4

2. PRODUCT OVERVIEW 5

2.1. INTRODUCTION 5
2.2. BLOCK DIAGRAM 5
2.3. PIN DESCRIPTION 5

3. COMMANDS 6

3.1. COMMAND CODE 6
3.2. COMMANDS DESCRIPTION 6

4. TRANSACTION SEQUENCE DESCRIPTION 7

4.1. TRANSACTION SEQUENCE DIAGRAM 7
4.2. TRANSACTION SEQUENCE DESCRIPTION 7

5. MEMORY ORGANIZATION AND ACCESS RIGHT 9

6. DATA INTEGRITY 12

1. Features

- **RF interface**
  - Compliant with ISO/IEC 14443-A
  - Contactless transmission of data and supply (no battery needed)
  - Operating frequency: 13.56MHz
  - Fast communication baud rate: 106Kbit/s
  - Contactless transmission of data and supply (no battery needed)
  - Operating distance: up to 100mm (depending on antenna geometry)
  - Half duplex communication protocol using handshake
  - Encryption algorithm compatible with M1 standard
  - Typical transaction time: ＜100ms
- **EEPROM**
  - 1024x8bit EEPROM memory
  - Organized in security separated 16 sectors supporting multi-application use.
  - User flexible defines assess conditions for each memory block.
- **High security**
  - Mutual three pass authentication
  - High security level data communication
  - Each sector has its own two secret files for systems using key hierarchies.
- **Arithmetic capability: increase and decrease.**
- **High Reliability**
  - Endurance: 100,000cycle
  - Data Retention: 10 Years

2. Product Overview

2.1. Introduction

FM11RF08 is the contactless card IC according to ISO14443 Type A development by Shanghai FuDan Microelectronics Co., Ltd. This device has 1K x 8bits EEPROM organization. The maximum communication range between the reader antenna and contactless card is approximately 10 cm.

FM11RF08 also has a very high security performance with the encryption and communication circuit, and is a true multi-application smart card with the functionality of a processor card realized with hardware logic. So FM11RF08 can be especially tailored to meet the requirements of a payment card which can be used for ticketing systems in public transport and comparable applications.

The Contactless smart card contains three components: FM11RF08 chip、antenna and the card base with PVC (or PET) material. No battery is needed. When the chip is positioned in proximity of the coupling device antenna, the high speed RF communication interface allows transmitting data with 106-Kbit/s.

2.2. Block Diagram

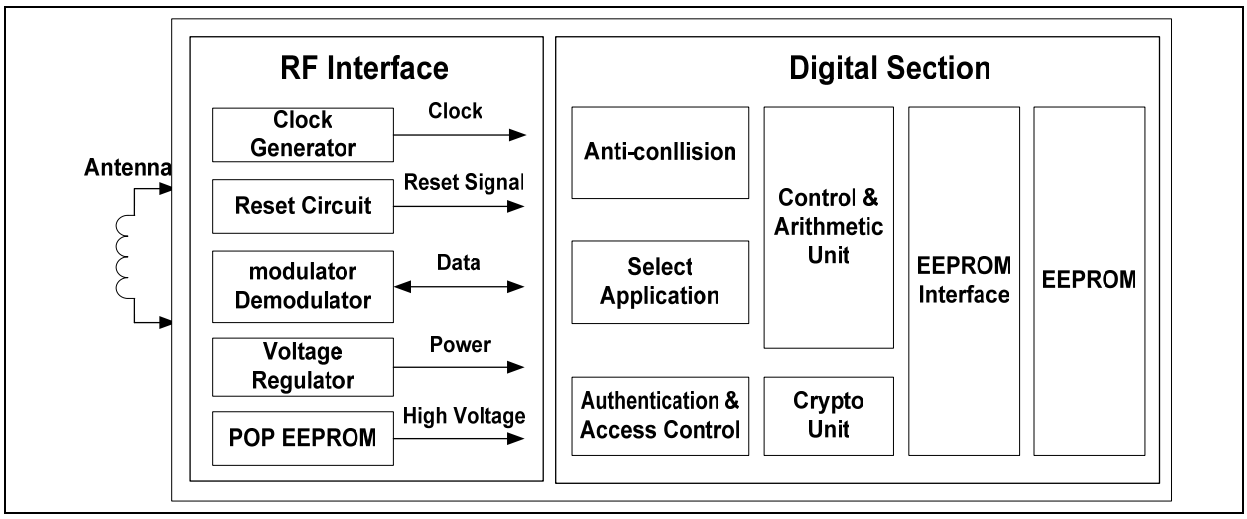

Figure 2-1 FM11RF08 Block Diagram

2.3. Pin Description

PIN	SYMBOL	TYPE	DESCRIPTION
1	IN1	input/output	Antenna interface 1
2	IN2	input/output	Antenna interface 2

Table 2-1 FM11RF08 Pin Description

3. Commands

3.1. Command Code

Commands	Code（HEX）
Request std	26
Request all	52
Anti-collision	93
Select Card	93
Authentication.Ia	60
Authentication.Ib	61
Read	30
Write	A0
Increment	C1
Decrement	C0
Restore	C2
Transfer	B0
Halt	50

Table 3-1 FM11RF08 Command Code (HEX)

3.2. Commands Description

Answer to Request: Look for card in operating area. ‘Request Std’ means looking for card which is not set to halt, ‘Request All’ means looking for all cards which are in operating area.

Anti-collision: It means selecting only one card if there is one card or several cards in operating area.

Select Card: It means setting up the communication with the selected card after the anti-collision command.

Authentication: Before visiting memory, the user must verify if the operation is legal by coherence of cipher in RWD and cipher in card.

Read: Read 16 bytes of one block.

Write: Write data to one block.

Increment: Increment a certain value to numerical block, store the result in register.

Decrement: Decrement a certain value to numerical block, store the result in register.

Restore: Read contents of numerical block to register.

Transfer: Write contents of register to numerical block.

Halt: Card is set to halt.

4. Transaction Sequence Description

4.1. Transaction sequence Diagram

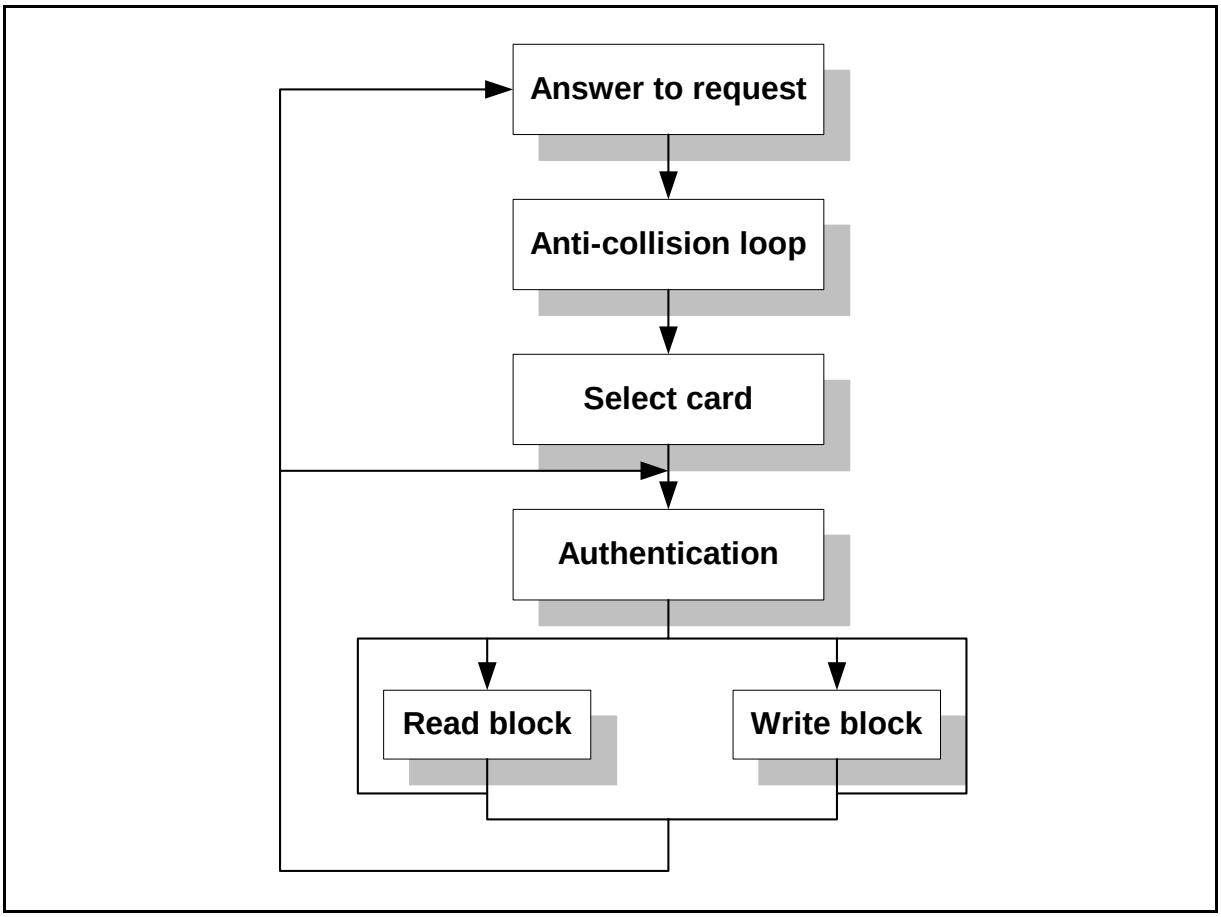

Figure 4-1 FM11RF08 Transaction Sequence Diagram

4.2. Transaction Sequence Description

Answer to Request: The type of a card defines the communication protocol and the communication baud rate between RWD and card. When a card is in the operating range of a RWD, the RWD continues communication with the appropriate protocol, specified by the type of a card.

Anti-collision Loop: If there are several cards in the operating range of RWD they can be distinguished by their different serial numbers and one selected for further transactions. The unselected cards return to the standby mode and wait for a new Answer to Request and Anti-collision loop.

Select Card: After selection of a card, the card returns the Answer to Select code (SAK).

3 Pass Authentication: After Selection of a card, RWD specifies the memory location of the following memory access and use the corresponding key for the 3 Pass Authentication procedures. Any communication after authentication is performed via stream cipher encryption.

Read/Write:
After authentication of the following operations may be performed:

READ: Read one block

WRITE: Write one block

DECREMENT: Decrements the contents of one block and stores the result in the data-register.

INCREMENT: Increments the contents of one block and stores the result in the data-register.

TRANSFER: Write the contents of the data-register to one block

RESTORE: Stores the contents of one block in the data-register

Halt: Pause operation

5. Memory Organization and Access Right

The FM11RF08 has integrated an 8K bits EEPROM which is split into 16 sectors with 4 blocks. One block consists of 16 bytes each.

The structure of memory is shown below:

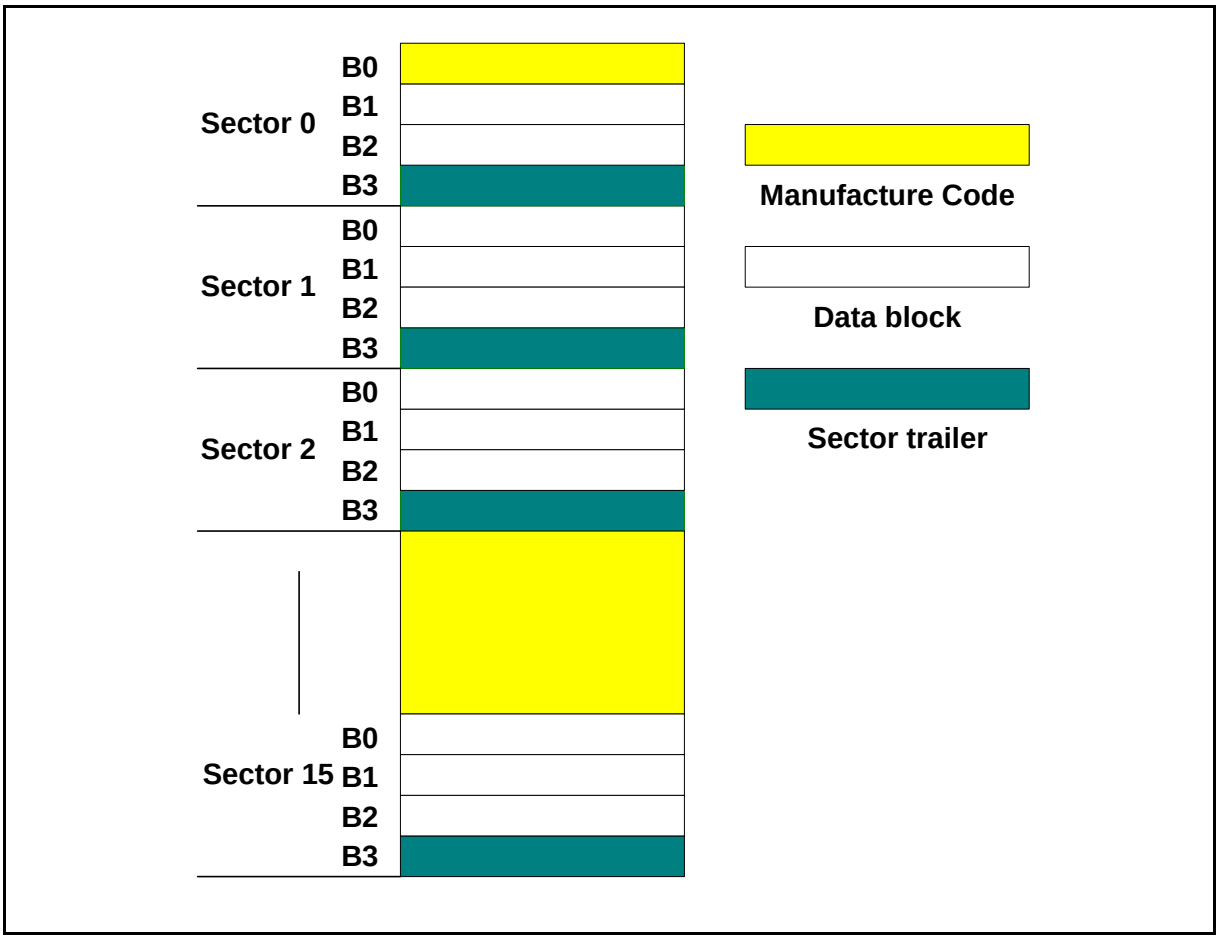

Figure 5-1 FM11RF08 Memory Organization

The fourth block of any sector contains access KEYA (6 bytes).an optional KEYB (6 bytes) and the access conditions for the four blocks of that sector (4 bytes). The other blocks of the sector serve as common data blocks. The first block of the memory is reserved for manufacturer data like 32 bit serial number. This is a read only block. In many documents it is named “block0”.

The structure of block3 is shown below:

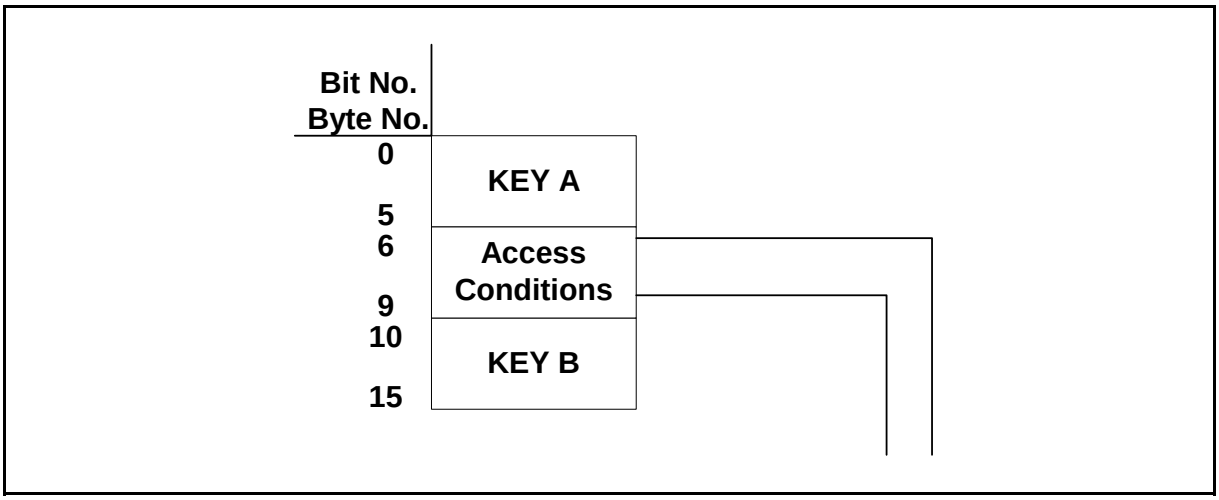

Figure 5-2 FM11RF08 Structure of Block 3

Memory organization:

Bit7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
C2X3_b	C2X2_b	C2X1_b	C2X0_b	C1X3_b	C1X2_b	C1X1_b	C1X0_b
C1X3	C1X2	C1X1	C1X0	C3X3_b	C3X2_b	C3X1_b	C3X0_b
C3X3	C3X2	C3X1	C3X0	C2X3	C2X2	C2X1	C2X0
BX7	BX6	BX5	BX4	BX3	BX2	BX1	BX0

Note:

b stands for inversion e.g.:C2X3_b=INV(C2X3)

X stands for sector No.(0~15)

Y stands for block No.(0~3)

C stands for control bit

B stands for reserve bit

Access condition for the Block 3 (X=0-15)

			KEYA	KEYA	Access Con	Access Con	KEYB	KEYB
C1X3	C2X3	C3X3	read	Write	Read	Write	read	Write
0	0	0	never	KEYA|B	KEYA|B	Never	KEYA|B	KEYA|B
0	1	0	never	Never	KEYA|B	Never	KEYA|B	Never
1	0	0	never	KEYB	KEYA|B	Never	never	KEYB
1	1	0	never	Never	KEYA|B	Never	never	Never
0	0	1	Never	KEYA|B	KEYA|B	KEYA|B	KEYA|B	KEYA|B
0	1	1	Never	KEYB	KEYA|B	KEYB	never	KEYB
1	0	1	Never	Never	KEYA|B	KEYB	never	Never
1	1	1	Never	Never	KEYA|B	Never	never	Never

Note: KEY A|B means KEY A or KEY B;

Never means can't perform the function.

Access condition for Data Blocks (X=0-15 sectors, y=0-2 block of each sector)

C1XY	C2XY	C3XY	Read	Write	Increment	decr, transfer, restore
0	0	0	KEYA|B	KEYA|B	KEYA|B	KEYA|B
0	1	0	KEYA|B	Never	Never	Never
1	0	0	KEYA|B	KEYB	Never	Never
1	1	0	KEYA|B	KEYB	KEYB	KEYA|B
0	0	1	KEYA|B	Never	Never	KEYA|B
0	1	1	KEYB	KEYB	Never	Never
1	0	1	KEYB	Never	Never	Never
1	1	1	Never	Never	Never	Never

6. Data Integrity

Following mechanisms are implemented in the contactless communication link between RWD and card to ensure very reliable data transmission.

- Anti-collision
- 16bit CRC per block
- Parity bits for each byte
- Bit count checking
- Bit coding to distinguish between “1”, “0”,and no information
- Channel monitoring (Protocol sequence and bit stream analysis)