

Attention Please!

The information describes the type of component and shall not to be considered as assured characteristics. For questions on technology, delivery and prices please contact Shanghai Fudan Microelectronics Co., Ltd in Shanghai, representatives in Shenzhen and Hong Kong.

Shanghai:

Technical Support:

Tel: (021) 6565 5050-169

Fax: (021) 6565 9112

Shenzhen:

Tel: (0755) 8335 0611

Fax: (0755) 8335 9011

Hong Kong:

Tel: (852) 2116 3288 2116 3338

Fax: (852) 2116 0882

CONTENTS.....	PAGE
1 FEATURES.....	4
1.1 Typical Transaction Time.....	4
2 BLOCK DIAGRAM.....	4
3 FUNCTION DISCRPTION.....	5
3.1 Transaction Sequence.....	5
3.1.1 Answer to Request.....	5
3.1.2 Anticollision Loop.....	5
3.1.3 Card Selection.....	5
3.1.4 3 Pass Authentication.....	6
3.1.5 Read/Write.....	6
3.2 Commands Aggregation.....	6
3.3 Data Integrity.....	6
3.4 Security.....	7
3.5 Memory Organization and Access Condition.....	7
3.5.1 Memory Organization.....	7
3.5.2 Access Condition.....	8
4 PACKAGE AND DIMENSIONS.....	9
4.1 Package.....	9
4.2 Dimensions.....	9

32kBits Contactless RF Card Chip FM11RF32

FM11RF32 is the contactless RF card chip developed by shanghai Fudan Microelectronics Co., Ltd. It takes 0.6 m CMOS EEPROM processing technology. The chip has 4K×8Bits EEPROM organization, and is a true multi-application RF card with hardware logic, it also has a very high security performance with the encryption and application circuit. FM11RF32 can be especially applied in ticketing systems of public transport and other concerned fields.

1 FEATURES

- ◆Compatible with ISO/IEC 14443 Type A
- ◆4096×8bit EEPROM memory, no battery.
- ◆13.56MHZ operating frequency
- ◆106Kbaud data communication rate
- ◆Operating distance (up to 100mm)
- ◆Half duplex communication protocol using handshaking
- ◆High security level data communication
- ◆Organized in security separated 64 sectors supporting multi-applications
- ◆Each sector has its own two secret files for systems using key hierarchies.
- ◆Access to memory zones for flexible user defined by a variety of access conditions.
- ◆Arithmetic capability: increase and decrease.
- ◆More than 100,000 read/write cycle
- ◆Data retention of 10 years

1.1 Typical Transaction Time

- ◆ Identification of a card 3ms
- ◆ Read Block (16bytes) 2.5ms(excl. Authentication)
- ◆ Write Block +Control Read 12ms(excl. Authentication)
14ms(incl. Authentication)
- ◆ Typical Transaction <100ms

2 BLOCK DIAGRAM

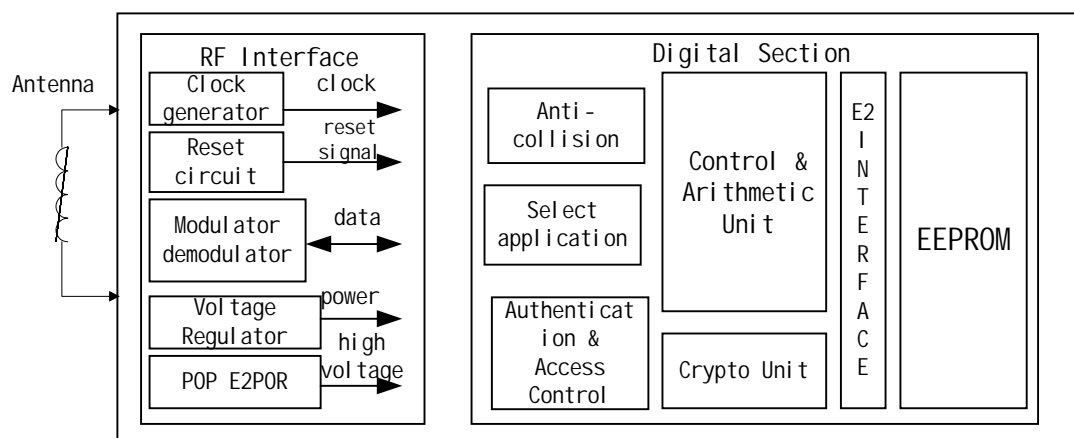


Fig1 Block Diagram

The electronic unit comprises just an antenna (coil) and an ASIC (FM11RF32) and no more

external components.

3 FUNCTION DESCRIPTION

3.1 Transaction sequence:

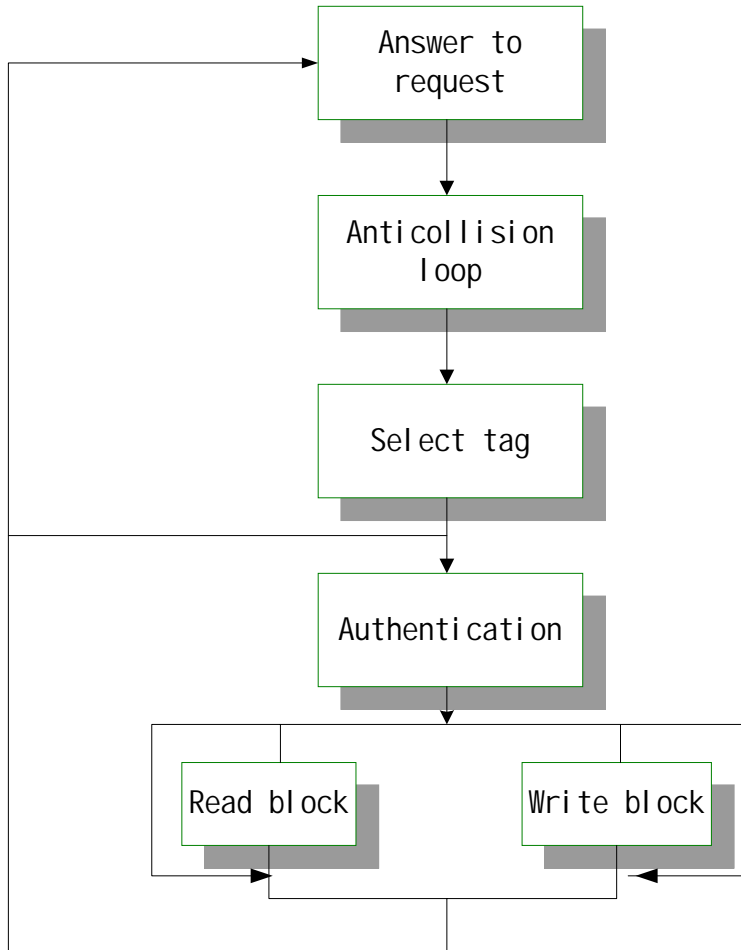


Fig 2 Transaction Sequence

3.1.1 Answer to Request:

FM11RF32 defines the communication protocol and the baudrate between PCD and card. When a card is in the operating range of a PCD, the RW then communicates with the appropriate protocol to verify the type of a card.

3.1.2 Anticollision Loop:

An anti-collision loop allows to operate more than one card in the field simultaneously. The anti-collision algorithm selects each card individually and ensures that the execution of a transaction with a selected card is performed correctly without data corruption resulting from other cards in the field.

3.1.3 Card Selection:

After a card selection, the selected card returns the Answer To Select Code (SAK).

3.1.4 3-Pass Authentication:

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

3.1.5 Read/Write:

After authentication, the following operations may be performed:

READ	read one block
WRITE	write one block
DECREMENT	decreases the contents of one block and stores the result in the data-register
INCREMENT	increases the contents of one block and stores the result in the data-register
TRANSFER	writes the contents of the data-register to one block
RESTORE	reads the contents of one block to the data-register
Halt	pause operation

3.2 Commands aggregation:

Commands	Code
Request std	26
Request all	52
Anti-collision	93
Select card	93
Authentication. La	60
Authentication. Lb	61
Read	30
Write	A0
Increment	C1
Decrement	C0
Restore	C2
Transfer	B0
Halt	50

3.3 Data Integrity

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

- Anticollision
- 16 bit CRC per block
- 16 bit Parity Checking per block
- Bit count checking
- Bit coding to distinguish between “1”, “0”, and no information
- Channel monitoring (Protocol sequence and bit stream analysis)

3.4 Security:

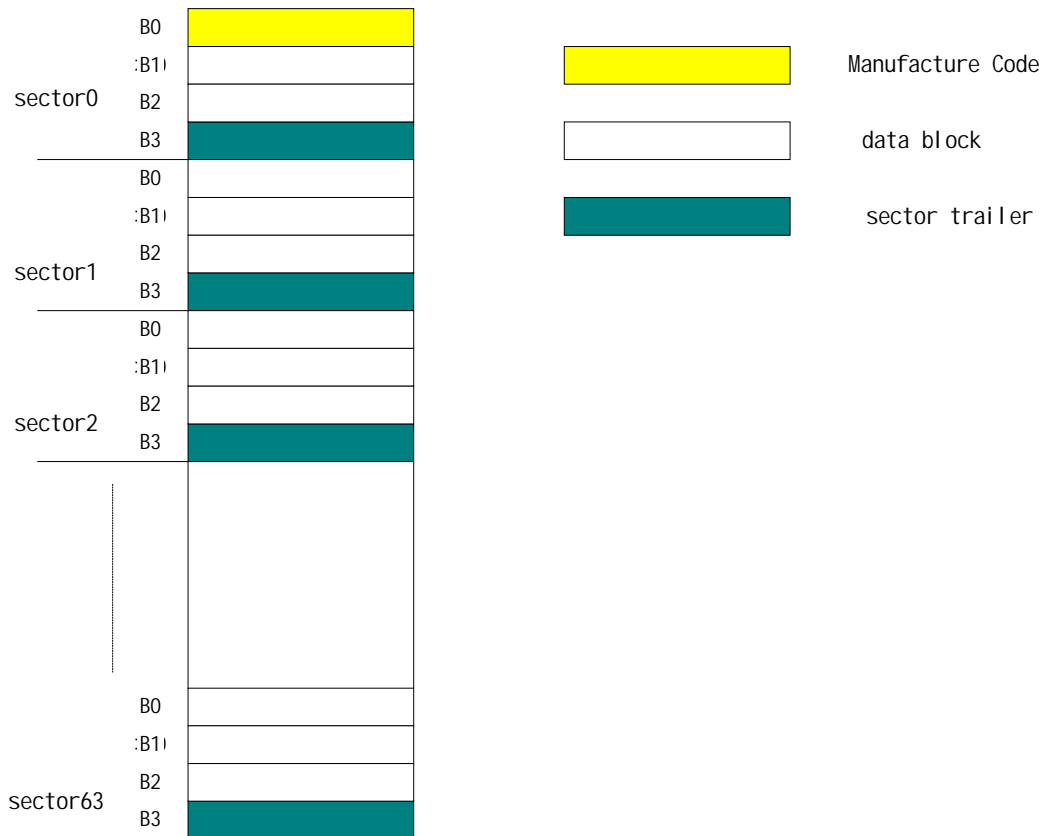
The FM11RF32 Card has very high security: 3 PASS Authentication must be through before read/write operation. Different cards with different serial numbers and cannot be altered to guarantee the uniqueness of each card. It is also with the function of Crypto-Data transfer, Key Transfer and Access Key Protection.

Keys in the cards are read protected but can be altered by who knows the actual keys. There are 64 sectors in the card; each sector has own keys (Key A, Key B). Two different keys for each sector support systems using key hierarchies, so FM11RF32 offers real multi-application.

3.5 Memory Organization and Access Conditions

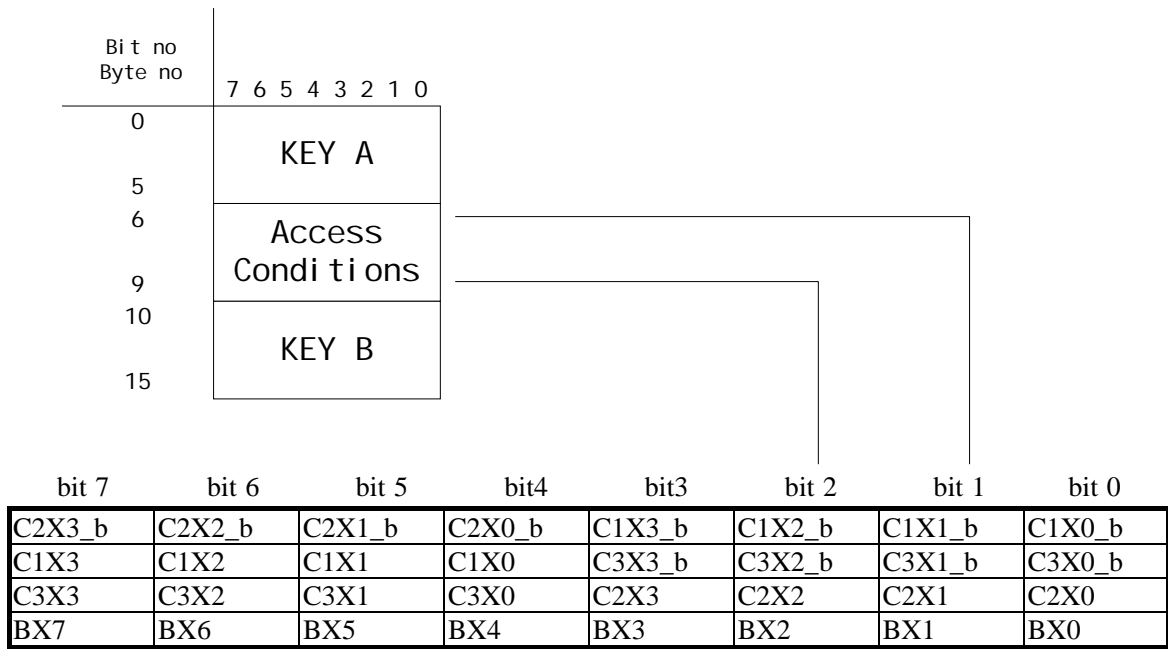
3.5.1 Memory Organization

The FM11RF32 has integrated a 32K bits EEPROM, which is organized to 64 sectors with 4 blocks. One block consists of 16 bytes



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

The structure of block3 is shown below.



b stands for inversion e.g.:C1X0_b=INV(C1X0)

X stands for sector No.(0~63)

Y stands for block No.(0~3)

3.5.2 Access condition

Access condition for the Sector Trailer(y=3)

			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 (y=0-2)

C1XY	C2XY	C3XY	Read	Write	Increment	Decrement, restore	transfer,
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	

4 PACKAGE AND DIMENSIONS

4.1 Package

Valid package is XOA II tape or chip for customer packaging.

4.2 Dimensions

MOA II tape package:

Module dimension: (4.75~4.90) mm×(4.95~5.10)mm, sickness: $0.38\text{mm} \leq T_{\text{TOTAL}} \leq 0.40\text{mm}$

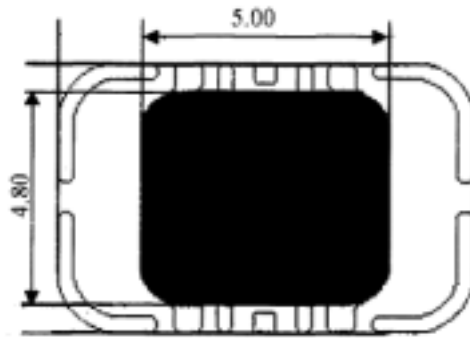


Fig 3 XOA2 Module Outline