FM11RF08S

8K bits Contactless Logic Security IC

Datasheet

Sep. 2020

Contents

1 Product Overview

1.1 Introduction

FM11RF08S (short for RF08S) is a logic security IC which based on ISO/IEC 14443A for the proximity contactless applications. It has excellent compatibility with all kinds of readers, enhanced RF performance and higher reliability of EEPROM.

Comparing with the old version chip RF08, RF08S's security and anti-decryption ability have been enhanced by fixing the weak points in the realization of the algorithm without losing of the functional compatibility. The communication distance has also been enhanced keeping the merit of compatibility with all kinds of readers.

1.2 Features

1.2.1 RF Interface

- ISO/IEC 14443-A
- Contactless transmission of data and supply energy (no battery needed)
- Operating distance: up to 10cm (depending on various parameters as e.g. field strength and antenna geometry)
- Operating frequency: 13.56 MHz
- Fast communication baud rate: 106Kbit/s
- 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

1.2.2 EEPROM

- 1024x8 bits EEPROM memory, Organized in security separated 16 sectors supporting multi-application use
- 10 years data retention
- Write endurance of 200,000 cycles

1.2.3 Security

- Unique identifier for each device, UID is unchangeable.
- Mutual three pass authentication
- High security level data communication
- Each sector has two keys separately
- User can defines assess conditions for each memory block flexibly
- Security and anti-crack ability have been enhanced comparing with the old version chip

1.3 Block diagram

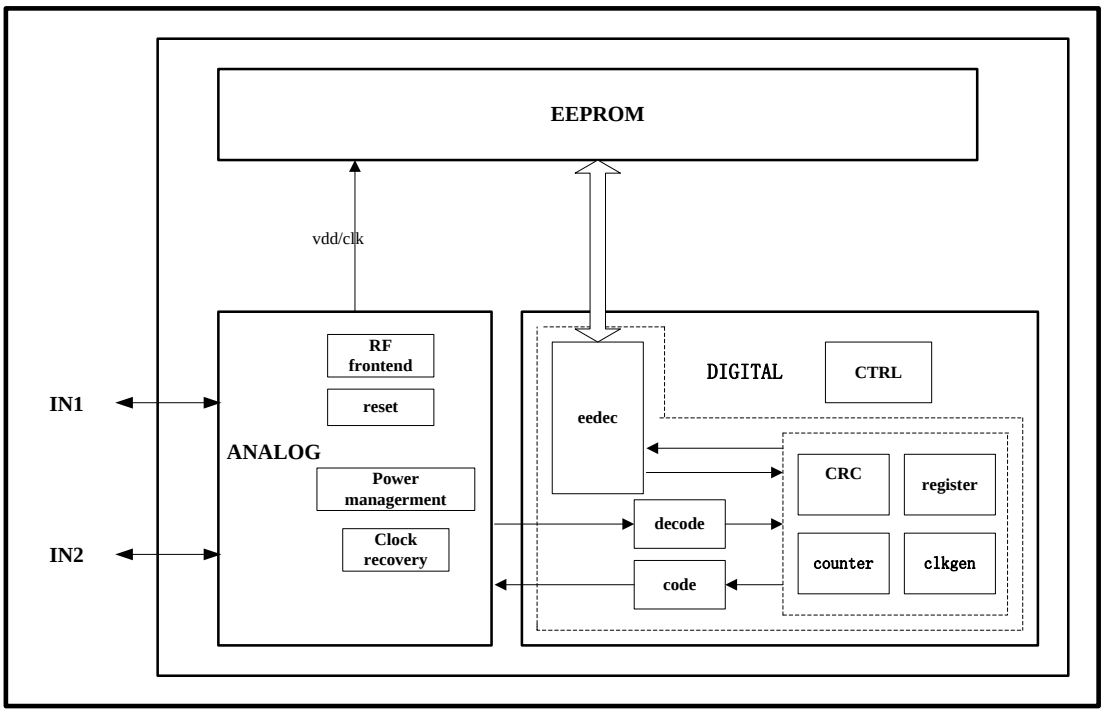

Figure 1-1 RF08S Block diagram

1.4 PIN description

Please consult Fudan Micro Electronics Company for the wafer datasheet.

1.4.1 Bare dies

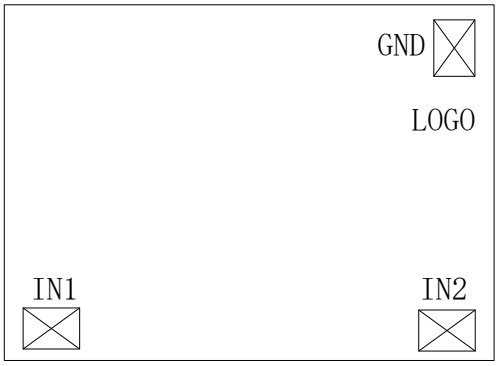

Figure 1-2 RF08S PIN description

Table 1-1 RF08S PIN description

Number	PIN name	PIN Description
1	IN1	antenna RF input
2	IN2	antenna RF input

3	GND	Ground of the chip

1.4.2 Bare dies with bump

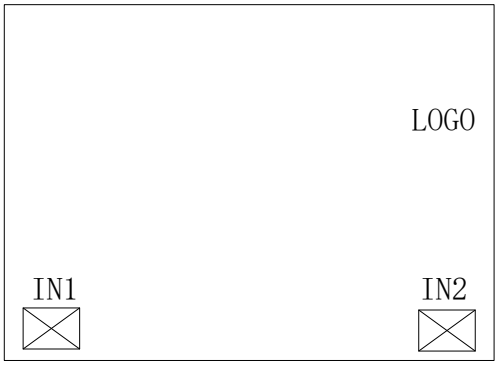

Figure 1-3 RF08S Bumping PIN description

Table 1-2 RF08S Bumping PIN description

Number	PIN name	PIN Description
1	IN1	antenna RF input
2	IN2	antenna RF input

2 Functional Description

2.1 General description

RF08S is a contactless card IC according to ISO14443 Type A which developed by Shanghai FuDan Microelectronics Co., Ltd. This device has a 1K x 8bits EEPROM.

RF08S also has a 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 RF08S can be especially tailored to meet the requirements of a payment card which can be used for ticketing systems in public transport and loyal card in consumption applications.

The Contactless smart card contains three components: RF08S 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 Memory organization and Access Right

The RF08S has an 8K bits EEPROM which has 16 sectors with 4 blocks. One block consists of 16 bytes each.

The structure of memory is shown below:

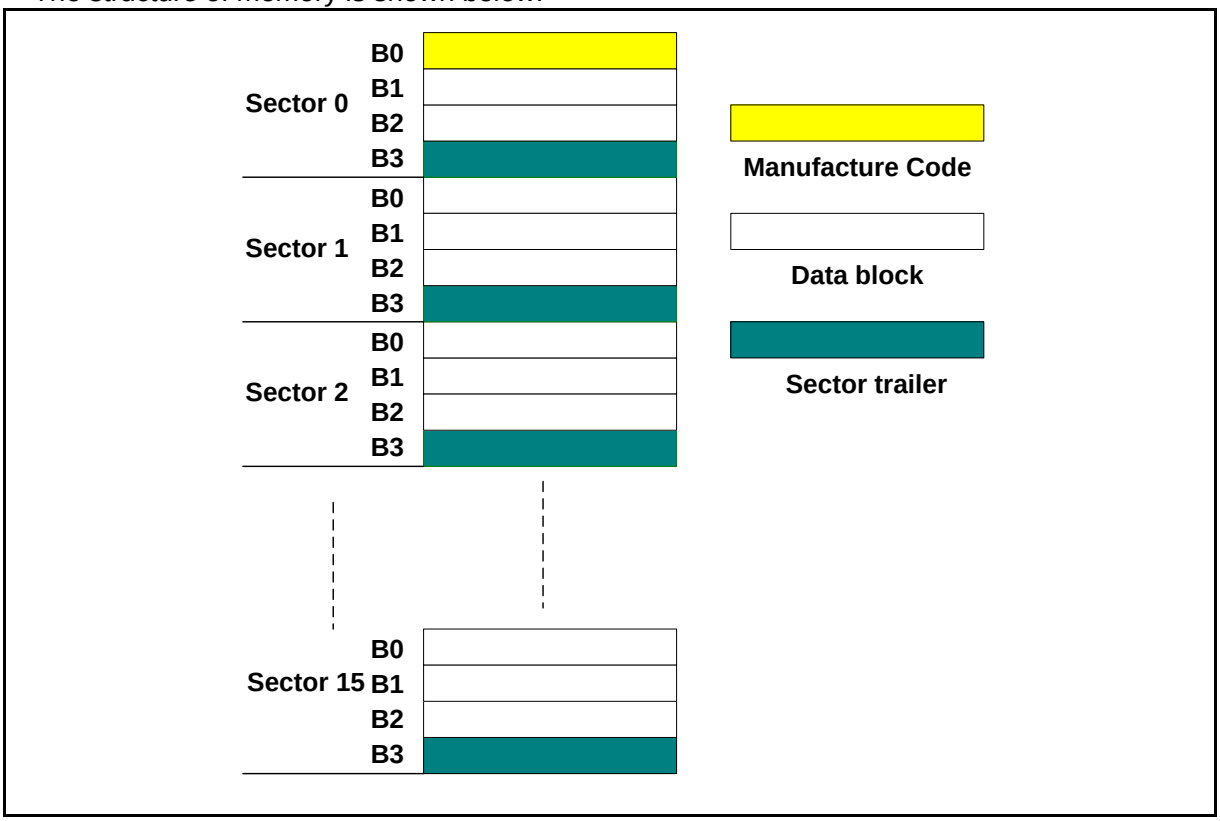

Figure 2-1 RF08S Memory Organization

The fourth block of every 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. It is a read only block “block0” generally.

The structure of block3 is shown below:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
KeyA						Access Bits				KeyB					

Figure 2-2 RF08S 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

C1XY	C2XY	C3XY	Read	Write	Increment	decr, transfer, restore
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

2.2.1 UID

The chip's 7 bytes UID is placed in the sector0 block0 of the memory.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
UID0~UID6							Chip Info								

Table 2-1 UID

According to ISO/IEC 14443-3, BCC0 is defined as CT⊕SN0⊕SN1⊕SN2. An ABBREVIATION CT stays for Cascade Tag byte (88h) and BCC1 is defined as SN3⊕SN4⊕SN5⊕SN6. SN0 holds the Manufacturer ID for Fudan Microelectronics (1Dh) according to ISO/IEC 14443-3 and ISO/IEC 7816-6 AMD.1.

2.2.2 Configuration of delivered ICs

RF08S is delivered with the following configuration by Fudan Micro:

• The UID is read only

• User data memory is not defined

Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	UID							Chip Info								
	1	00															
	2	00															
	3	FF						FF	07	80	69	FF					
1	0	00															
	1	00															
	2	00															
	3	FF						FF	07	80	69	FF					
15	0	00															
	1	00															
	2	00															
	3	FF						FF	07	80	69	FF					

Figure 2-3 Memory configuration

2.3 Transaction Sequence Description

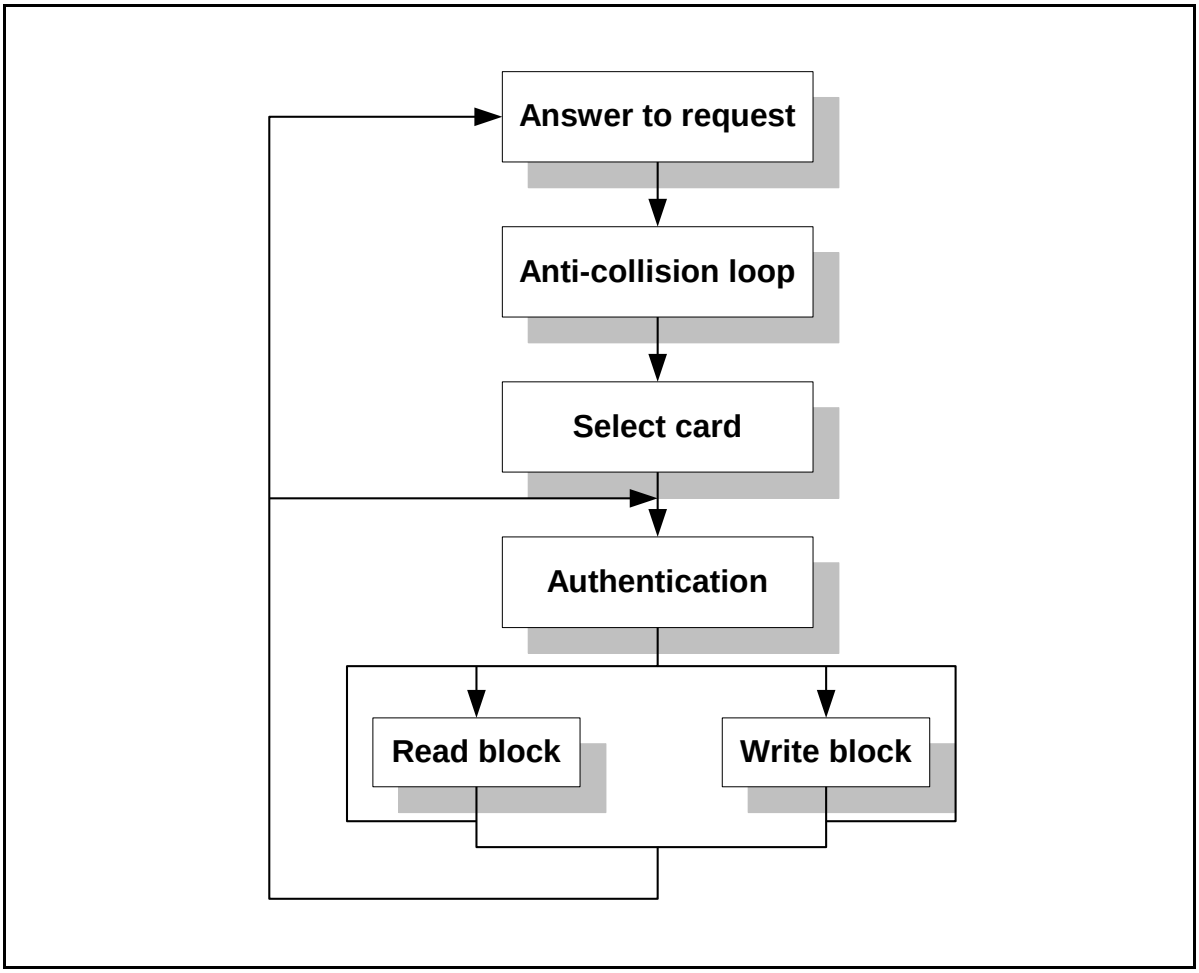

Figure 2-4 RF08S Transaction Sequence Diagram

Answer to Request: The type of a card defines the communication protocol and the communication baud rate between reader and card. When a card is in the operating range of a reader, the reader 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 reader 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, reader 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

2.4 Command set

The RF08S comprises the command set as described in following chapters.

NAME	CODE(HEX)
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

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 reader 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.

2.5 Data integrity

Following mechanisms are implemented in the contactless communication link between reader 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)

2.6 Security

The RF08S card has high security: 3PASS Authentication must be get through before read/write operation. Serial Numbers, which cannot be altered, guarantee the uniqueness of each card. 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 key. There are 16 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 RF08S offers real multi-application functionality.

RF08S's security and anti-crack ability have been enhanced by fixing the weak points in the realization of the algorithm without losing of the compatibility. There is no difference in using method of RF08S and RF08.

3 Characteristics

3.1 Limiting values

Symbol	Parameter	Conditions	Min	Max	Unit
T_{stg}	storage temperature	-	-55	+125	°C
I_I	input current（IN1 to IN2）	IN1 to IN2; RMS	-	30	mA
V_{ESD}	ESD （HBM）【3】	-	4	-	KV

Table 3-1 RF08S Limiting values【1】【2】

【1】：Stresses above one or more of the limiting values may cause permanent damage to the device.

【2】: This product includes circuitry specifically designed for the protection of its internal devices from the damaging effects of excessive static charge. Nonetheless, it is suggested that conventional precautions be taken to avoid applying greater than the rated maxima.

【3】：Human body model: C = 100 pF, R = 1.5 k. For ESD measurement, the IC was mounted in a CDIP8 package.

3.2 Normal Working Condition

Symbol	Parameter	Min	Typ	Max	Unit
T_A	Temperature	-40	+25	+85	°C
H_A	Operation Field strength	1.5		7.5	A/M

Table 3-2 RF08S normal working condition

3.3 Electrical characteristics

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
f_i	input frequency	【1】	13.553	13.56	13.567	MHz
C_i	input capacitance	Between IN1 and IN2【2】	13	15	17	pF

Table 3-3 Electrical characteristics

【1】 Bandwidth limitation (±7 kHz) according to ISM band regulations.

【2】 Measured with Agilent E5061B at 13.56 MHz and 0.707V RMS.

3.4 EEPROM characteristics

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
t_{ret}	retention time	T_{amb} = 55℃	10			year
$N_{endu(W)}$	write endurance	T_{amb} = 25℃	200,000			cycle

Table 3-4 EEPROM characteristics

4 Ordering information

Type Number	Wafer Type	Description
FM11RF08S-7B-WTB2	Bump Sawn Wafer	12 inch bump wafer (sawn, laser diced; 120 um thickness, without UV exposure, on film frame carrier; electronic fail die marking according to SECSII format)
FM11RF08S-7B-WTS5	Sawn Wafer	12 inch wafer (sawn, laser diced; 150 um thickness, on film frame carrier; electronic fail die marking according to SECSII format)