EM4170

125kHz CRYPTO READ/WRITE Contactless Identification Device

Description

The EM4170 is a CMOS integrated circuit intended for use in electronic Read/Write RF Transponders. The chip contains an implementation of a crypto-algorithm with 96 Bits of user configurable secret-key contained in EEPROM. It also provides a unique Device Identification of 32 bits that can never be modified as well as 94 bits of freely programmable USER-MEMORY. Bits 15 and 14 of word 1 are used as Lock-Bits. The memory can only be accessed for writing or erasing if these two bits have the contents "x0" as when they are delivered.
The memory can be unlocked by using the PIN-code command. In that case, the lock-bits are reset from the value "x1" to the value "x0".
The EM4170 transmits data to the transceiver by modulating the amplitude of the electromagnetic field, and receives data and commands in a similar way.
The coil of the tuned circuit is the only external component required, all remaining functions are integrated in the chip.

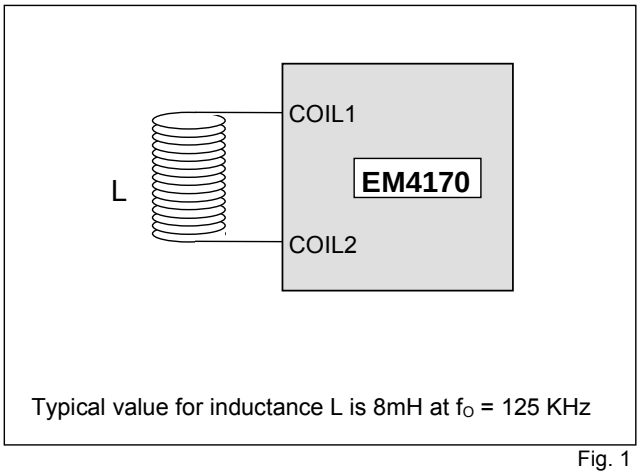
Features

- On Chip Crypto-Algorithm
- Two Way Authentication
- 96 bits of Secret-Key in EEPROM (unreadable)
- 32 bits of fix Device Identification
- 32 bits of PIN code (unreadable)
- 94 bits of USER_MEMORY (UM) with read access (OTP)
- Secret-Key programmable via CID-Interface
- Lock-Bits to inhibit programming
- Data Transmission performed by Amplitude Modulation
- Bit Period = 32 periods of carrier frequency
- 200pF on chip Resonant Capacitor (untrimmed)
- -40 to +85°C Temperature range
- 100 kHz to 150 kHz Field Frequency
- On chip Rectifier and Voltage Limiter
- No external supply buffer capacitance needed due to low power consumption

Typical Applications

- Anti-counterfeiting
- High security hands-free access control

Typical Operating Configuration



Typical value for inductance L is 8mH at f_O = 125 KHz

Fig. 1

System Principle

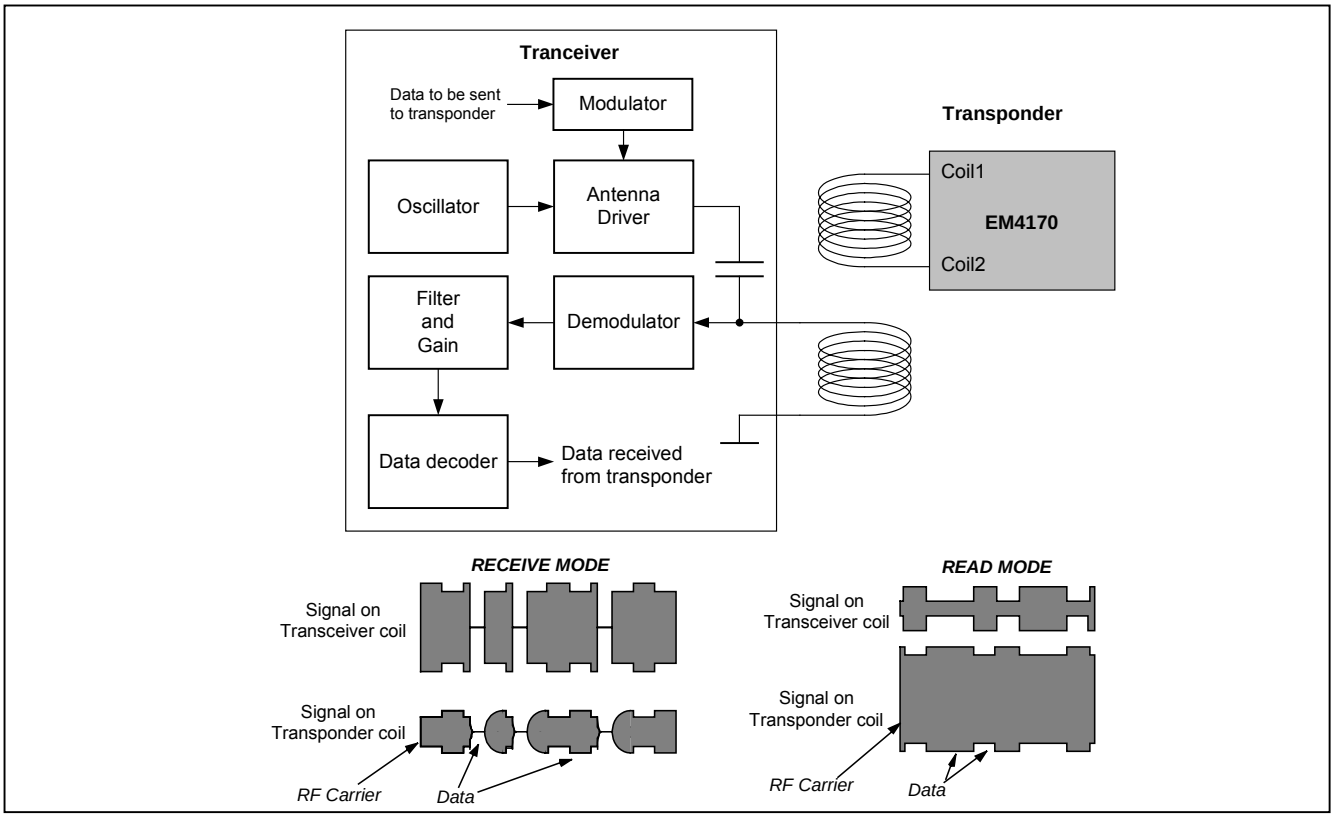


Fig. 2

Block Diagram

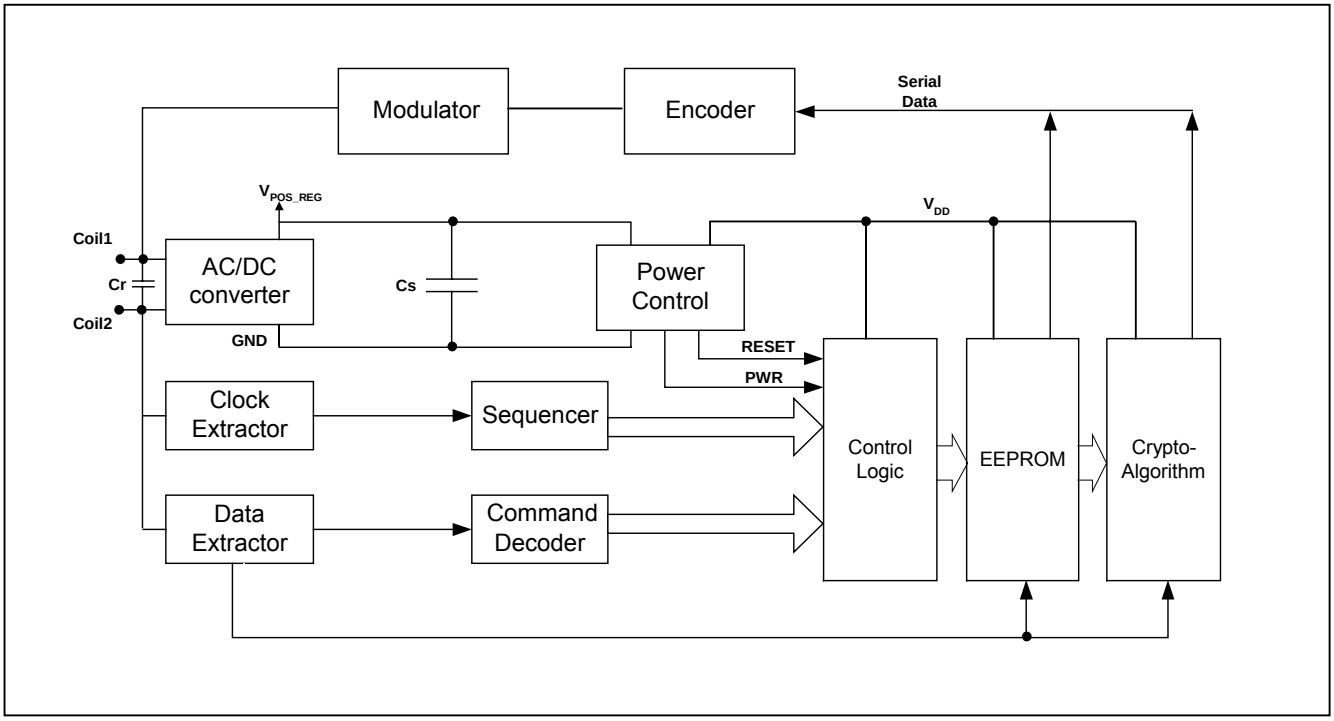


Fig. 3

Absolute Maximun Ratings

Parameter	Symbol	Min.	Max.	Units
Supply Voltage (Unregulated)	$V_{POS-REG}$	-0.3	9.5	V
Supply Voltage (regulated)	V_{DD}	-0.3	5.5	V
Voltage at remaining pins Excepted COIL1, COIL2	V_{PIN}	V_{SS} - 0.3	V_{DD} + 0.3	V
Storage temperature	T_{store}	-55	+ 125	°C
Electrostatic discharge (Mil-STD-883 C method 3015)	V_{ESD}	1000		V
Maximum Current induced on COIL1 and COIL2	I_{COIL}	-30	+ 30	mA

Operating Conditions

Parameter	Symbol	Min.	Typ.	Max.	Units
Operating Temperature	T_{OP}	-40	+25	+85	°C
Maximum coil current	I_{COIL}	-10		+10	mA
Frequency on Coil inputs	F_{COIL}	100	125	150	kHz

Handling Procedure

Stresses above these listed maximum ratings may cause permanent damage to the device. Exposure beyond specified electrical characteristics may affect device reliability

Electrical parameters and functionality are not guaranteed when the circuit is exposed to light.

This device has built-in protection against high static voltages or electric fields; however, anti-static precautions should be taken as for any other CMOS component. Unless otherwise specified, proper operation can only occur when all terminal voltages are kept within the supply voltage range.

Electrical Characteristics

$V_{DD} = V_{POS\_REG} = 2.5V$, $V_{SS} = 0V$, $f_{coil} = 125$ kHz Sine wave, $V_{coil} = 1V_{pp}$, $T_{op} = 25°C$ unless otherwise specified.

Parameter	Symbol	Conditions	Min.	Typ.	Max.	Units
Supply Voltage(unregulated)	$V_{POS-REG}$	V_{POS_REG} = max (note 1)			1)	V
Supply Voltage (regulated)	V_{DD}	Read Mode (note 2)	2.8	3.5	4.2	V
EEPROM read voltage	V_{RD}		2.0			V
EEPROM write voltage	V_{EE}		2.5			V
Supply current / read	I_{rd}	Read Mode V_{DD} =2.0V			5.0	µA
Supply current /write @25°C	I_{wr25}	Write Mode, V_{DD} =2.5V		30	38	µA
Supply current / write	I_{wr}	Write Mode, V_{DD} =2.6V -40°C<T<85°C			70	µA
Modulator voltage drop	V_{ON}	V_{Coil1} - V_{SS} and V_{Coil2} - V_{SS} I_{coil} = 100µA V_{Coil1} - V_{SS} and V_{Coil2} - V_{SS} I_{coil} = 5mA	0.30	0.45	0.60 2.50	V V
Resonnance Capacitor	C_r	10 kHz, 100 mV_{pp}	170	200	230	pF
Capacitor temp. coeff	TKC_r	-40°C to 85°C	-75		+75	ppm/K
Capacitor tolerance/wafer	$TOLC_r$		-2		+2	%
POR level high	V_{prh}	Rising Supply		2.0	2.4	V
POR level low	V_{prl}	Falling Supply		1.8	2.2	V
Clock extractor input min	V_{clkmin}	Min for clock extraction	0.6	0.36		V_{pp}
Clock extractor input max	V_{clkmax}	Max for clock extraction			50	mV_{pp}
EEPROM data endurance	N_{cy}	Erase all / Write all	100000			cycles
EEPROM retention	T_{ret}	Top = 55°C after 100'000 cycles (note 3)	10			years

Note 1 : Maximum voltage is defined by forcing 10mA on Coil1-Coil2
Note 2 : The circuit is not functional below the POR-level
Note 3 : Based on 1000 hours at 150°C

Timing Characteristics

Parameter	Symbol	Conditions	Min.	Typ.	Max.	Unit
Power on Reset Time	t_{por}				600	µs
Read Bit Period	t_{rdb}			32		periods
LIW/ACK/NACK pattern Duration	t_{patt}			160		periods
Duration of ID	t_{rID}			1536		periods
Divergency-Time	T_{div}			224		periods
Authentication-Time	t_{auth}			4224		periods
WRITE Access Time	t_{wa}			128		periods
EEPROM write time	t_{wee}			3072		periods
WRITE Access Time of the Lock Bits	t_{walb}	V_{DD}=3V		672		periods

RF periods represent periods of the carrier frequency emitted by the transceiver unit. For example, if 125kHz is used, the Read bit period would be: 1/125'000*32 = 256µs.

Functional Description

The EM4170 is supplied by means of an electromagnetic field induced on the attached coil. The AC voltage is rectified in order to provide a DC internal supply voltage. When the DC voltage crosses the Power-On level, the chip will enter the Standby Mode and expect commands. In Standby Mode a continuous sequence of Listen Windows (LIW) is generated. During this time, the crypto-Chip will turn to the Receive Mode (RM) if it receives a valid RM pattern. The chip then expects a command to enter the desired mode of operation.

Memory Organisation

The 256 bits EEPROM are organised in 16 words of 16 bits. Words 0 and 1 contain the USER_MEMORY_1 and the Lock-Bits LB1 and LB0. Words 12, 13, 14 and 15 contain the USER_MEMORY_2. Write-Mode can only be entered if LB0 = "0" (LB1= "X").
Words 2 and 3 contain the ID that can never be modified. Words 4 through 9 contain the 96 bits of secret key. These bits influence the crypto-algorithm but cannot be read directly. Words 11 and 12 contain the 32 bits of PIN-Code. These two words can be written when the lock bits are in unlocked state. They cannot be read out as for the secret key.

Memory Map

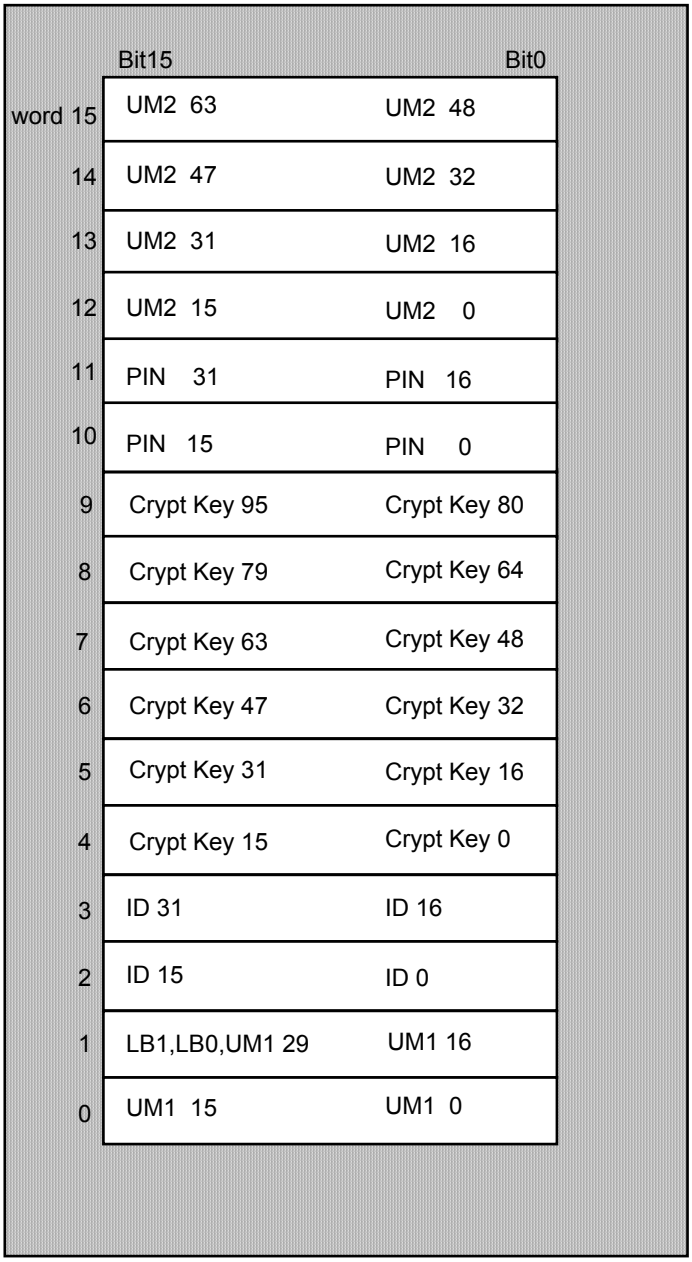


Fig. 4

Standby Mode
After a Power-On Reset and upon completion of a command, the chip will execute the Standby Mode, in which it will continuously send LIWs to allow the reader to issue commands. As every LIW has a duration of 160 periods of the RF field the reader can turn to Receive mode every 1.3ms at 125kHz.

Receive Mode
To change from Standby Mode to another operation the chip has to be brought into Receive Mode. To do this the Transceiver sends to the chip the RM pattern during the 32 clocks of modulated phase in a Listen Window (LIW). The EM4170 will stop sending data upon reception of a valid RM. The RM pattern consists of 2 bits "0" sent by the transceiver. The first "0" is to be detected during the 32 periods when the modulation is "ON" in the LIW. Next the EM4170 expects a command to specify the operation to be executed.

Commands
The commands are composed of 4 bits, divided into 3 data bits and 1 even parity bit (total amount of "1's" is even including the parity bit). There exist 6 different commands. Upon reception of an unknown command or a command with wrong parity the chip will immediately return into Standby Mode.

Commands

COMMAND BITS	*FUNCTION*
0 0 1 1	ID-MODE
0 1 0 1	UM-MODE-1
0 1 1 0	AUTHENTICATION
1 0 1 0	WRITE WORD
1 0 0 1	SEND PIN
1 1 1 1	UM-MODE-2

First bit Recieved

Parity bit

Fig. 5

ID Mode
After reception of the command including the parity the chip sends a header consisting of 12 Manchester coded '1's followed by 4 Manchester coded '0's. Then the chip sends the 32 Bits of ID contained in words 3 and 2 of the EEPROM once without parity starting with the MSB of word 3. After completion the chip returns to Standby-Mode.

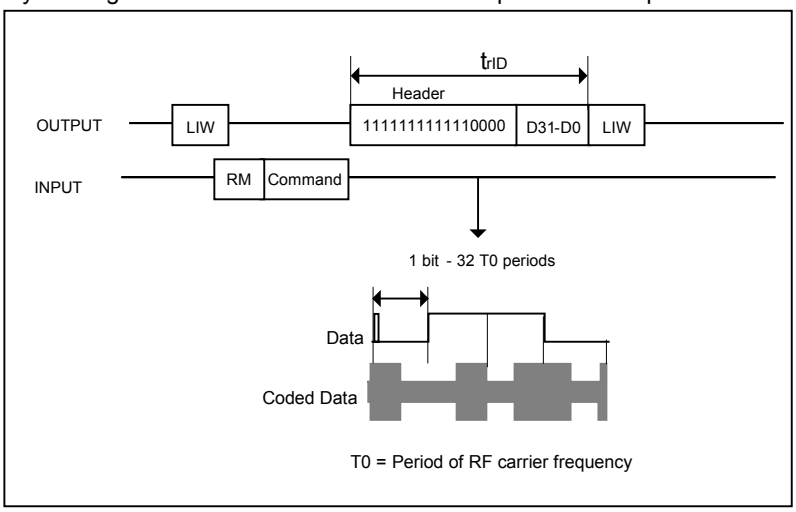


Fig. 6

UM-MODE-1
In UM-MODE-1 the chip sends LB1 and LB0 followed by the 30 Bits of UM1 starting with the MSB following the same procedure as in ID-MODE. After completion the chip returns to Standby Mode

Authentication

In this mode the chip first receives the 56 bits of random number followed by a certain number of divergency bits that the reader should send as "0" followed by 28 Bits of cipher_1 (f(RN)) as authentication of the lock. The chip decides if the authentication is accepted. In this case the EM4170 sends a header (12 Manchester coded '1's followed by 4 Manchester coded '0's). Next 20 Bits of cipher_2 (g(RN)) are sent. Else it sends a single NAK. Upon completion of this command the EM4170 returns to Standby Mode.

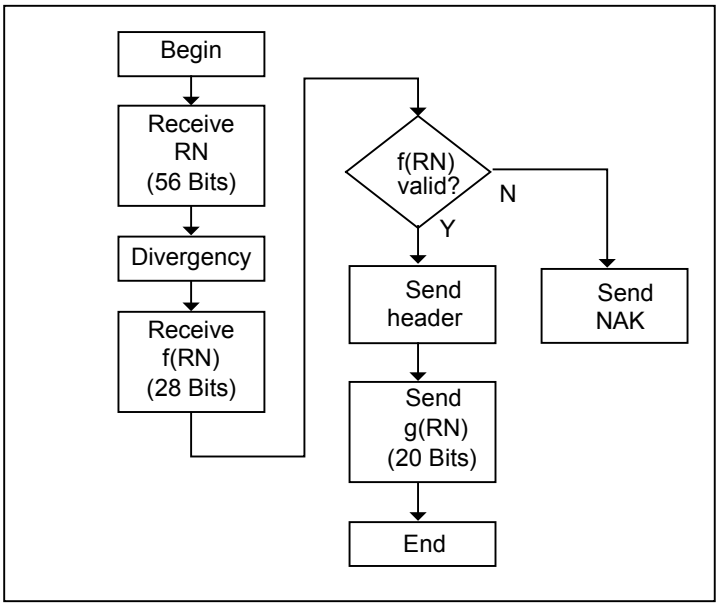


Fig. 7

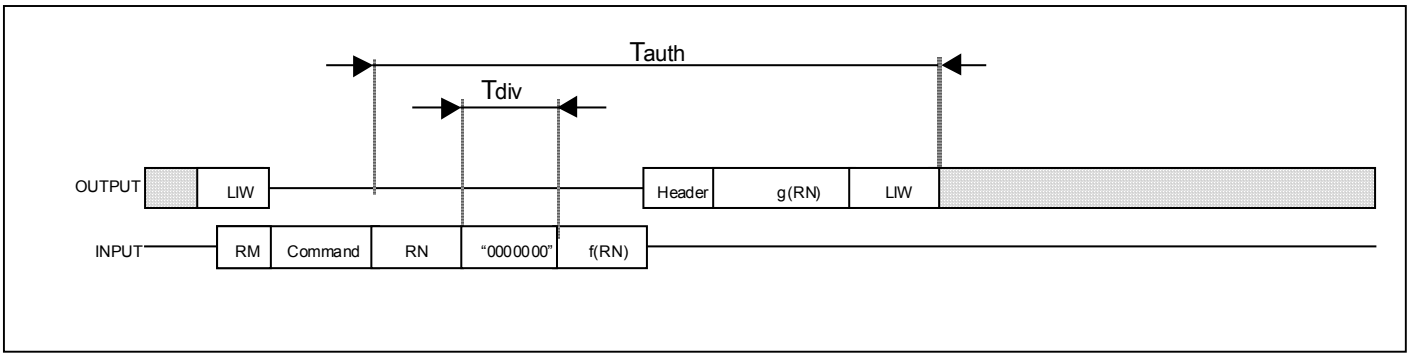


Fig. 8

Write Word

The Write Word command is followed by the address and data. The address consists of a 5 bit block containing 4 data bits and 1 even parity. The data consists of 4 times 5 bit blocks, each block consisting of 4 data bits and 1 associated even parity bit. One additional block consists of 4 column parity bits and a trailing zero (refer to fig 10).

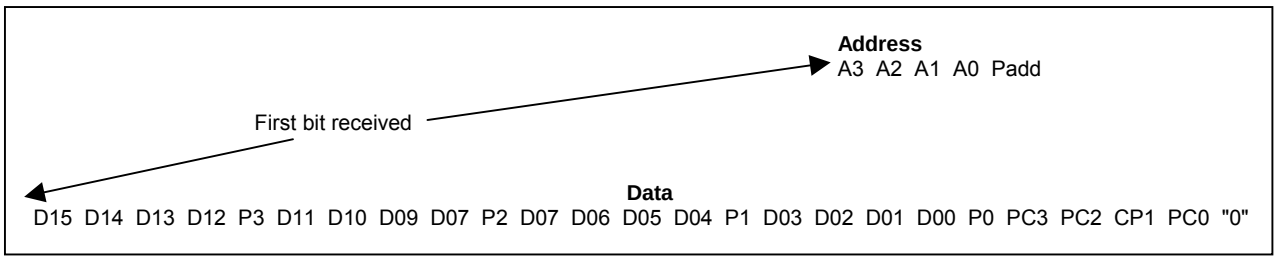


Fig. 9

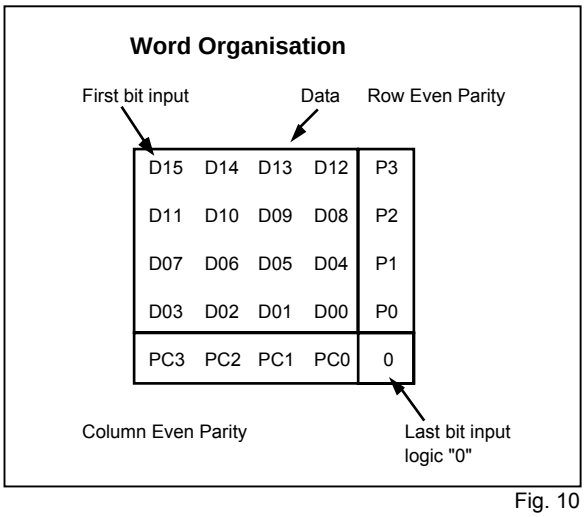


Fig. 10

After reception of the write command, the address and the data, the EM4170 will check the parity and the Lock-Bits. If all the conditions are fulfilled, an Acknowledge pattern (ACK) will be issued, and the EEPROM writing process will start. At the end of programming the chip will send an Acknowledge pattern (ACK). If at least one of the checks fails, the chip will issue a No Acknowledge pattern (NAK) instead of ACK and return to the Standby Mode.
The EM4170 might also return to the Standby Mode without sending back a NAK if the incoming data is corrupted and/or inconsistent.
As there is no check of the power supply before writing, the system has to assure that there is enough power received by the tag (V_{DD}≥2.6V), when performing the write command.

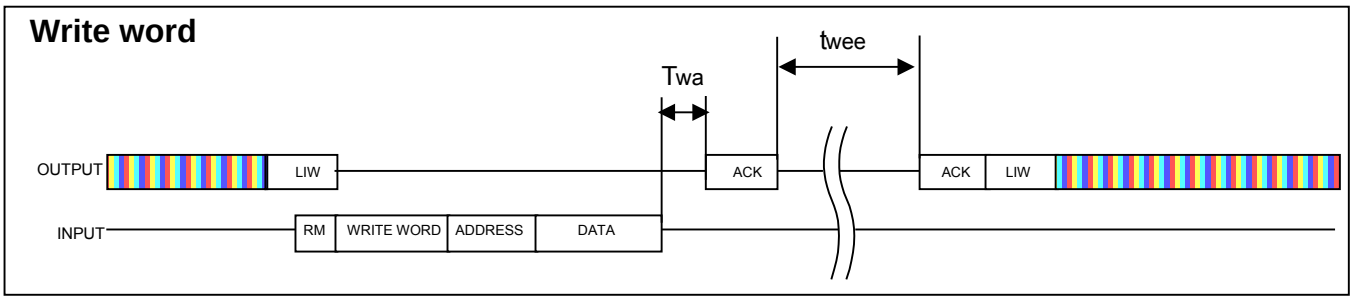


Fig. 11

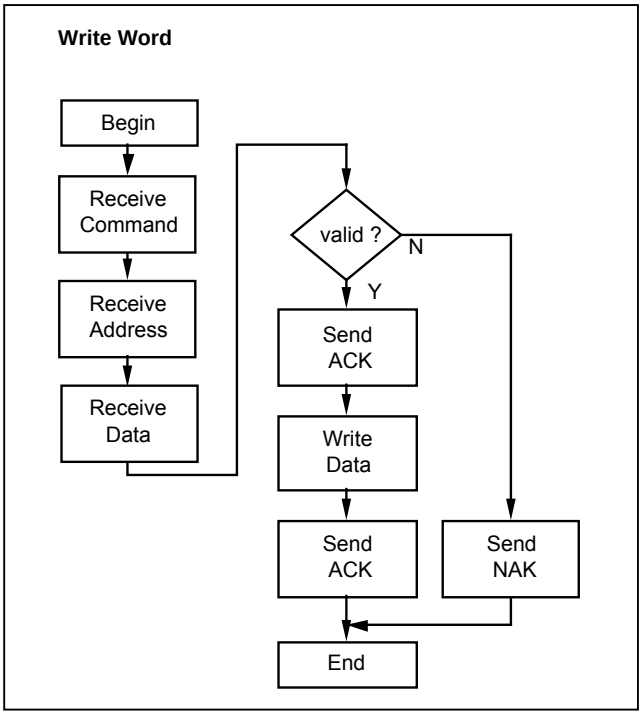


Fig. 12

SEND PIN

In this mode after reception of the command, the chip receives the 32 bits of the ID and the 32 bits of the PIN. If the received data are valid, the chip will answer an ACK and write the lock bit LB0 to 0; then it will send back the header (12 « 1 » and 4 « 0 ») followed by the ID. Then the chip returns to Stand-by Mode. If the ID or the PIN are not valid, the chip sends back a NACK and return to Stand-by Mode.

The EM4170 might also return to Stand-by Mode without sending back a NAK if the incoming data is corrupted and / or inconsistent.

As there is no check of the power supply before writing, the system has to assure that there is enough power received by the tag (V_{DD}≥2.6V), when performing the send pin command.

After a successful SEND PIN command, it is recommended to check the content of the word 1 with the UM1 command.

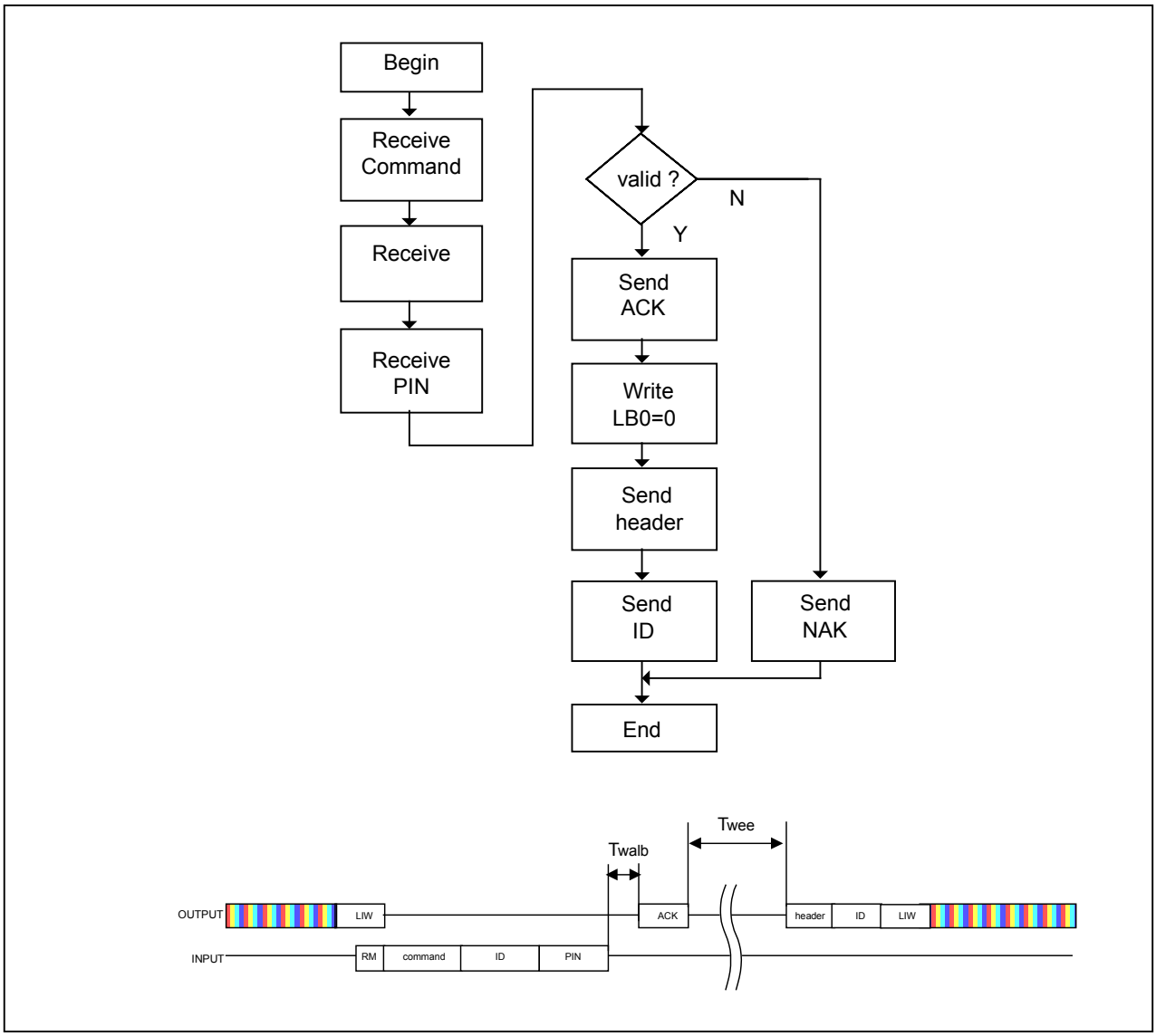


Fig. 13

UM-MODE-2

In UM-Mode-2 the chip sends the 64 bits of UM2. It starts with MSB of Word 15 and finishes with LSB of Words 12. The chip is using the same procedure than in ID-Mode, by sending the header before the data bits.

After completion the chip returns to Stand-by Mode.

Power On Reset
When the EM4170 with its attached coil will enter an electromagnetic field, the built in AC/DC converter will supply the chip. The DC voltage is monitored and a Reset signal is generated to initialise the logic. The power On Reset is also provided in order to make sure that the chip will start issuing LIWs and be ready to accept commands with a sufficient DC power level. An hysteresis is provided to avoid improper operation at limit level.

AC/DC Converter and Voltage Limiter
The AC/DC converter is fully integrated on chip and will extract the power from the incident RF field. The internal DC voltage will be clamped to avoid high internal DC voltage in strong RF fields.

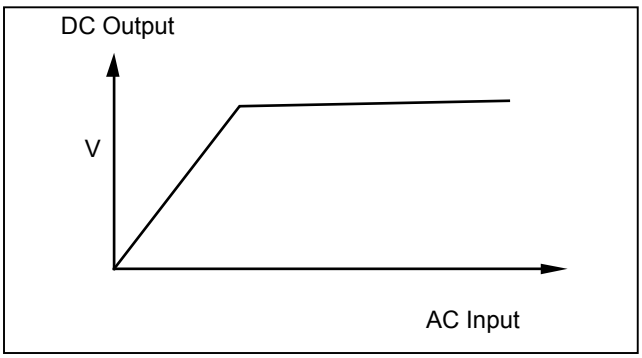


Fig. 14

Clock Extractor
The Clock extractor will generate a system clock with a frequency corresponding to the frequency of the RF field. The system clock is fed into a sequencer to generate all internal timings.
The clock extractor is optimised for power-consumption, sensitivity and noise-suppression. As the input signal is subject to a large dynamic range due to the amplitude modulation, the clock-extractor may miss clocks or add spurious clocks close to the edges of the RF-envelope. This de-synchronisation will not be larger than ± 1 clocks per Bit and must be taken into account when developing reader software.

Data Extractor
The transceiver-generated field will be amplitude modulated to transmit data to the EM4170. The Data extractor demodulates the incoming signal to generate logic levels, and decodes the incoming data.

Modulator
The Data Modulator is driven by the serial data outputted from the memory or the Crypto-Logic which is Manchester encoded. The modulator will draw a large current from both coil terminals, thus amplitude modulating the RF field according to the memory data.

Communication from Transponder to the Transceiver (READ MODE)
The EM4170 modulates the amplitude of the RF field to transmit data to the transceiver. The data is output serially from the EEPROM and Manchester encoded.

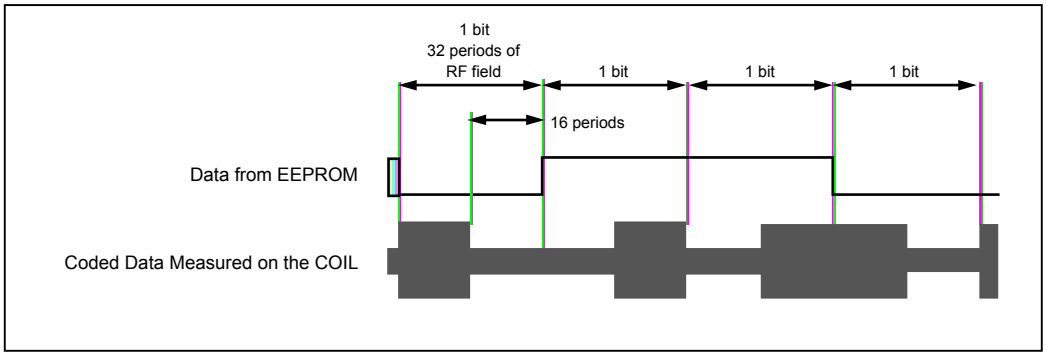


Fig. 15

The EM4170 uses different patterns to send status information to the transceiver. Their structure cannot be confused with a bit pattern sequence. These patterns are the Listen Window (LIW) to inform the transceiver that data can be accepted,

the Acknowledge (ACK) indicating proper communication and end of EEPROM write, and the No Acknowledge (NAK) when something is wrong.

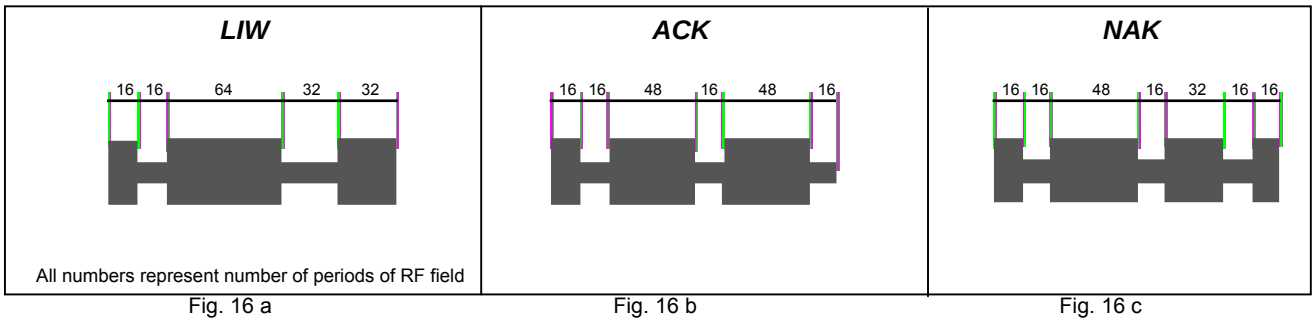


Fig. 16 a Fig. 16 b Fig. 16 c

Communication from the Transceiver to the Transponder (RECEIVE MODE)

The EM4170 can be switched to the Receive Mode ONLY DURING A LISTEN WINDOW. The Transceiver is synchronised with the incoming data from the transponder. During the phase when the chip has its modulator "ON" (32 periods of RF), the transceiver has to send a bit "0". At reception of the first "0", the chip stops immediately the LIW sequence and expects then another bit "0" to switch to receive mode. The transceiver and the chip are now synchronised and further data is sent with a bit rate of 32 periods of the RF field.

The EM4170 turns "ON" its modulator at the beginning of each frame of 32 clock periods corresponding to one bit. To send a logic "1" bit, the transceiver continues to send clocks without modulation. After 16 clocks, the modulation device of the EM4170 is turned "OFF" allowing recharge of the internal supply capacitor. To send a logic "0" bit, the transceiver stops sending clocks (100% modulation) during the first half of a bit period (first 16 periods). The transceiver must not turn "OFF" the field earlier than clock 1 of a bit period. It is recommended to turn "OFF" the field after 4 clocks of the bit period. The field is stopped from clock 5 to 16 of the bit period, and then turned "ON" again for the remaining 16 periods.

To ensure synchronisation between the transceiver and the transponder, a logic bit set to "0" has to be transmitted at regular intervals. The RM pattern consists of two bits set to "0" thus allowing initial synchronisation.

While the transceiver is sending data to the transponder, two different modulations will be observed on both coils. During the first 16 clocks of a bit period, the EM4170 is switching "ON" its modulation device causing a modulation of the RF field. This modulation can also be observed on the transceiver's coil. The transceiver to send a bit "0" will switch "OFF" the field, and this 100% modulation will be observed on the transponder coil.

Communication from the Transceiver to the Transponder

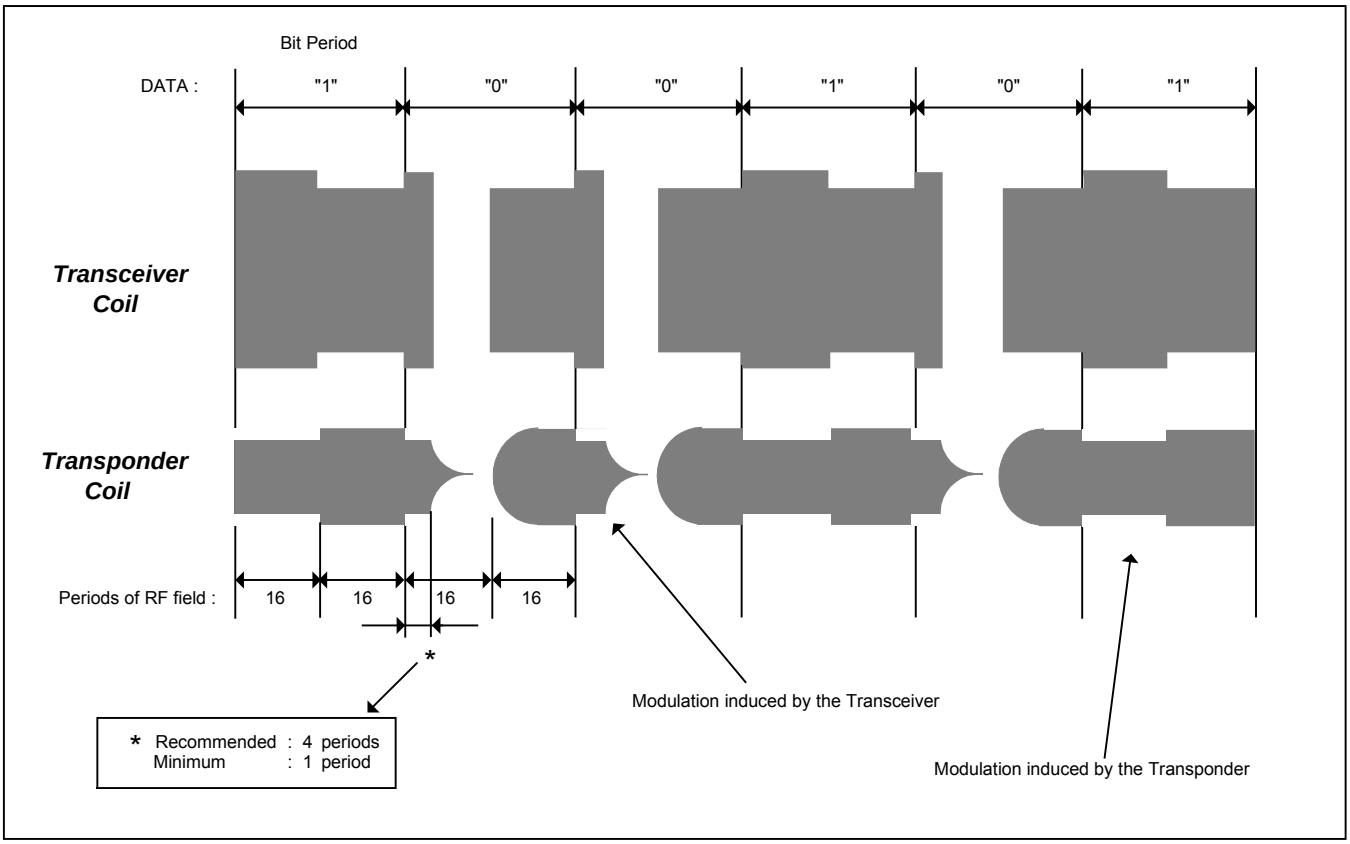


Fig. 17

Pad Assignment

Pin	Name	Description
1	COIL1	Coil connection
2	VPOS	Unregulated positive supply
3	VDD	Positive supply
4	TEST_OUT	Test pad output
5	TEST	Test pad with pull down
6	TEST_CLK	Test pad with pull down
7	VSS	Negative supply
8	COIL2	coil connection

Pad Location

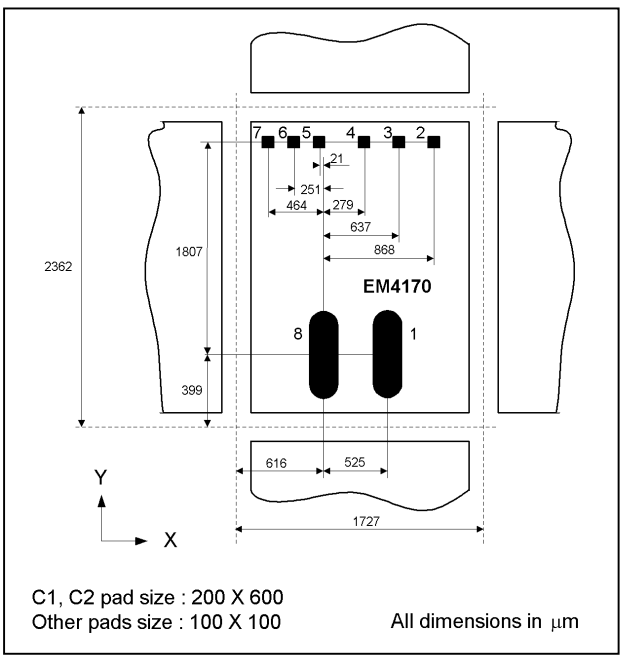
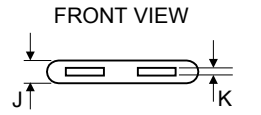
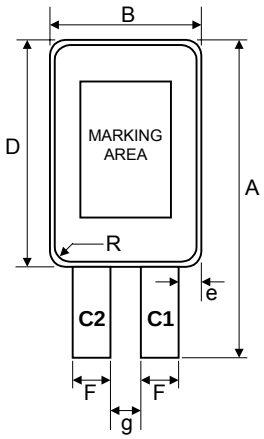


Fig. 18

Packages

CID Package



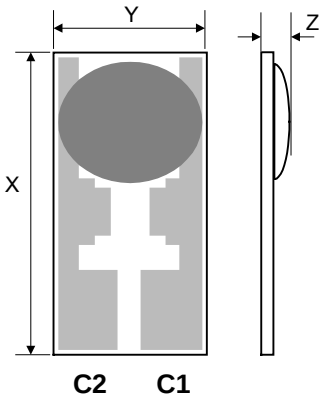


SYMBOL	MIN	TYP	MAX
A	8.2	8.5	8.8
B	3.8	4.0	4.2
D	5.8	6.0	6.2
e	0.38	0.5	0.62
F	1.25	1.3	1.35
g	0.3	0.4	0.5
J	0.42	0.44	0.46
K	0.115	0.127	0.139
R	0.4	0.5	0.6

Dimensions are in mm

Fig. 19

PCB Package



SYMBOL	MIN	TYP	MAX
X		8.0	
Y		4.0	
Z			1.0

Dimensions are in mm

Fig. 20

Ordering Information

Part Number	Bit Coding	Cycle Bit	Package / Die Form	Delivery Form / Bumping
EM4170A5WW11	Manchester	32	unsawn wafer, 11mils thickness	No bump
EM4170A5WW11E	Manchester	32	unsawn wafer, 11mils thickness	Gold bumps
EM4170A5WS7	Manchester	32	sawn wafer on frame, 7mils thickness	No bump
EM4170A5WT11E	Manchester	32	die on sticky tape, 11mils thickness	Gold bumps
EM4170A5CI2LB	Manchester	32	CID package, 2 pins (length 2.5mm)	Tape
EM4170A5CB2RC	Manchester	32	PCB package	Bulk

For other packages, please contact EM Sales

Product Support

Check our Web Site under Products/RF Identification section.
Questions can be sent to cid@emmicroelectronic.com

A special development kit exists with embedded co-crypt processor. This tool is mandatory to use authentication command.