32-bit Secure Element MCU

Device

- CW9008 – VQFN32-5x5

Process

- 55nm

Key Features

- ARM cortex-M0 MCU Core
  - 100MHz maximum frequency
  - 0.9 DMIPS/MHz
  - Single-cycle multiplication and hardware division
- Memories
  - 256K bytes Flash memory

    1 Kbyte per page, main array 256 pages, information array 64bytes.

    Endurance 100K cycles, 10 years data retention
  - 64K bytes of SRAM
  - OTP 1K bytes
- Peripheral DMA functions
- NVIC (Nested Vectored Interrupt Controller, 32 external interrupt input)
- System Power Management Controller (SPMC) with internal regulator supports multiple power modes including:
  - ➢ RUN
  - ➢ HSRUN
  - ➢ STOP
  - ➢ VLPR
  - ➢ VLPS/SUSPEND
- Embedded hardware crypto engine with 60MHz frequency
- PUF (Physical Unclonable Function) key, total 2K bits, 256 bits for UID number
- TRNG (True random Number Generator)
- Embedded PLL, 8MHz input, x12 96MHz output or x15 120MHz output
- Embedded oscillator 8MHz & 10KHz (SRC)
- Embedded LDO 3.3v to 1.2V, typical 50mA output capability
- Package
  - QFN type, pin-out and pin number depend on applications

Peripheral & Communication interface

- USB 2.0 full speed device
- SPI master

- SPI slave
- I2C master
- I2C slave
- UART
- FTM (Flex Timer Module) or PWM (Pulse Width Modulation)
- GPIO
- TRGMUX (Triger Multiplexer module)
- Programmable CRC5-32

Hardware crypto engine

• Public Key Cryptography (signature, key agreement)

› ECDSA: FIPS 186-3 Elliptic Curve Digital Signature Algorithm

› ECDH: NIST SP800-56A Elliptic Curve Diffie-Hellman

› NIST standard P256 Elliptic Curve

› SM2: GM/T 0003-2012

• Private Key Cryptography (message authentication code, key wrapping)

› AES128/192/256: FIPS PUB 197

› SM4: GM/T 0002-2012

› Mode of operation: NIST SP800-38A/B/C/D/E

› key wrapping : NIST SP800-38F

• Hash Function (data integrity, message authentication code, key derivation)

› SHA224/256/384/512, SHA512_224/256: FIPS 180-4

› SM3: GM/T 0004-2012

› HMAC: FIPS 198-1

› KDF: KDF-HMAC, KDF-CMAC

Table of Contents

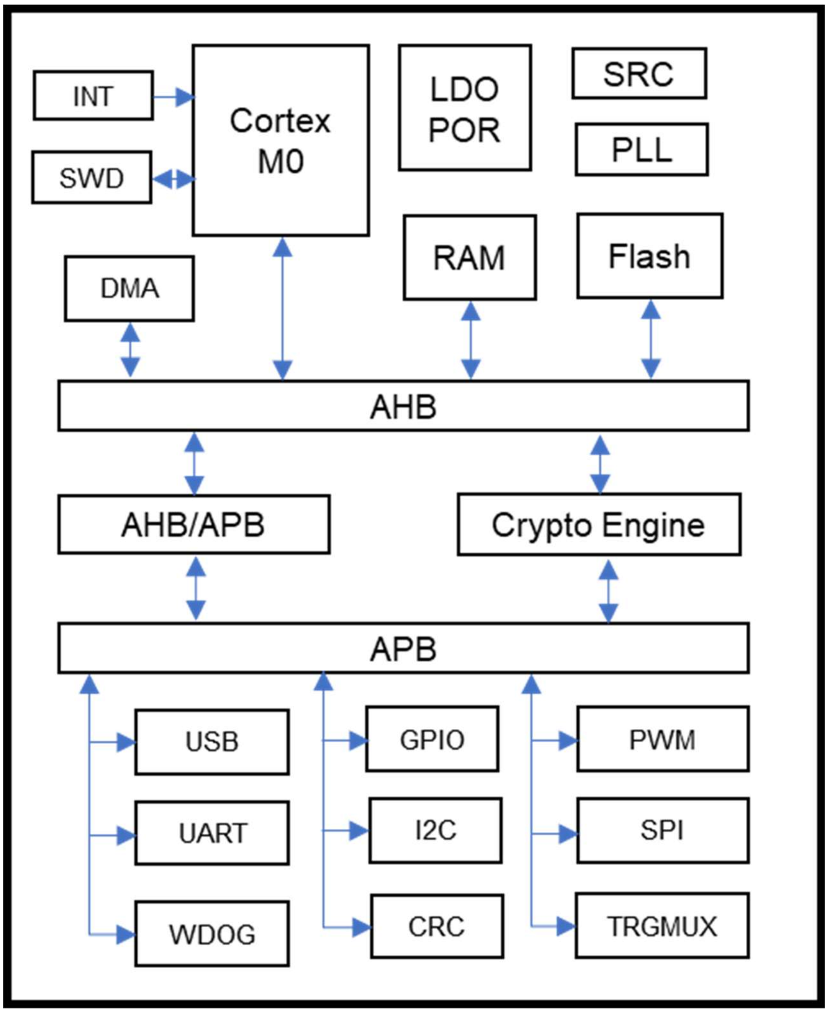
1. Overview

The CW9008 is a low-power secure microcontroller to provide multiple layers of advanced physical security. It is available in QFN type package, depend on interface application.

The microcontroller also contains a hardware encryption engine, allowing applications to quickly respond to challenges and authenticate other devices using standards-based cryptography. A true-hardware random-number generator (TRNG) is available for general application use, such as key generation, challenge generation, and random padding. Low level drivers and reference codes are available as well.

Multiple communication interfaces are implemented: an integrated USB transceiver and serial interface engine make USB applications extremely low cost; also included are an SPI and I2C.

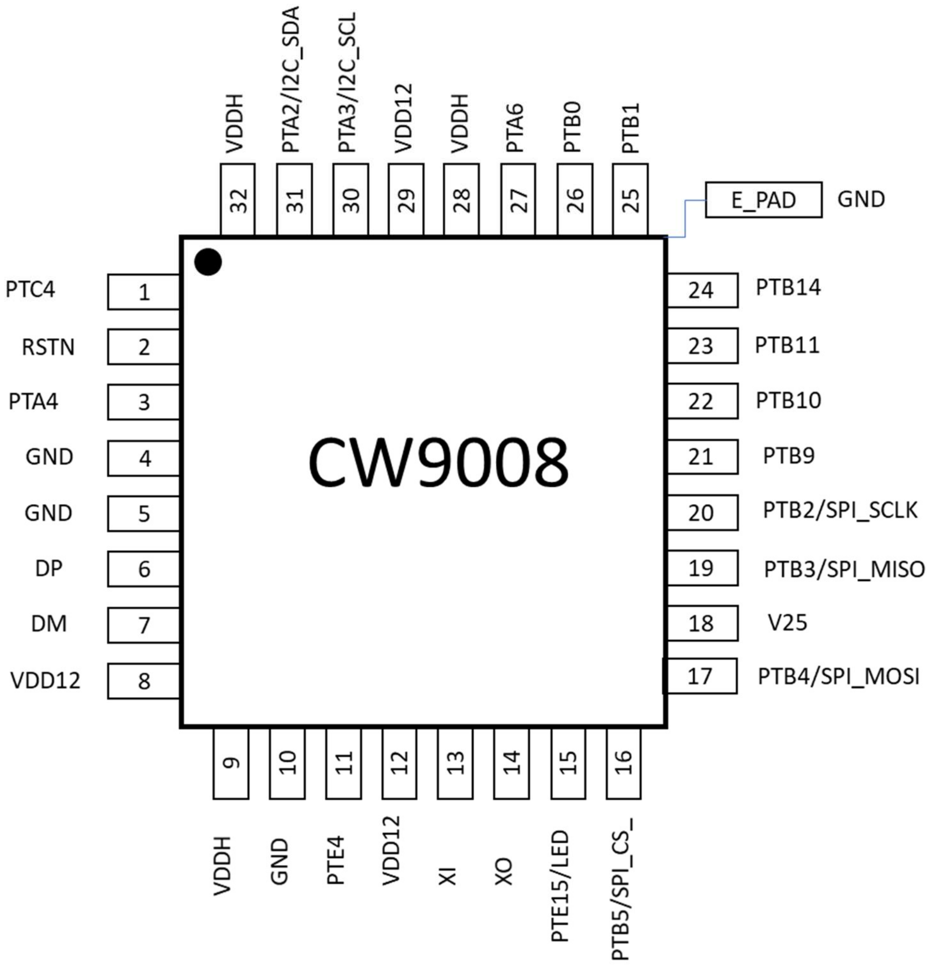
Function block diagram



2. Pin Description

2.1 Pin Configuration

Pinout of CW9008



2.2 Pin Definition

PWR: Power or ground pin

A I: Analog input pin

A O: Analog output pin

A I/O: Analog input/output pin

I: Digital input pin

O: Digital output pin

I/O: Digital input/output pin

CW9008 pin description

Pin No.	Symbol	Pin Type	Description
1	PTC4	I	Reserved
2	RSTN	I	Reset. External reset signal, active low, with weak internal pull-up resistor.
3	PTA4	O	Reserved
4	GND	PWR	Connect ground
5	GND	PWR	Connect ground
6	DP	A I/O	USB D+ signal, analog IO pin
7	DM	A I/O	USB D- signal, analog IO pin
8	VDD12	PWR	Core power 1.2V
9	VDDH	PWR	IO power 3.3V Power input.
10	GND	PWR	Connect ground
11	PTE4	I/O	GPIO function
12	VDD12	PWR	Core power 1.2V.
13	XI	A I	X’tal input, analog input.
14	XO	A O	X’tal output, analog output
15	PTE15	I/O	GPIO function
16	PTB5/ SPI_CS_	I/O	SPI master chip select output or SPI slave chip select input. The SPI chip select signal, active low.
17	PTB4/ SPI_MOSI	I/O	Master output slave input data signal. SPI data from master to slave.
18	V25	PWR	OTP power 2.5V input
19	PTB3/	I/O	Master input slave output data signal. SPI data from slave to master.

	SPI_MISO		
20	PTB2/ SPI_SCLK	I/O	SPI master clock output or SPI slave clock input. Only support SPI mode 0.
21	PTB9	I/O	GPIO function
22	PTB10	I/O	GPIO function
23	PTB11	I/O	GPIO function
24	PTB14	I/O	GPIO function
25	PTB1	O	Reserved
26	PTB0	I	Reserved
27	PTA6	I/O	GPIO function
28	VDDH	PWR	IO power 3.3V Power input.
29	VDD12	PWR	Core power 1.2V
30	PTA3/SCL	I/O	I2C clock signal.
31	PTA2/SDA	I/O	I2C data signal.
32	VDDH	PWR	X’tal output, analog output
E_PAD	GND	PWR	Need connect package E_PAD to system ground

3. Peripheral & Communication interface descriptions

3.1 USB 2.0 full speed device

Integrate USB 2.0 full speed PHY and USB device controller
Control endpoint 0, with IN/OUT buffer 64 bytes
Interrupt IN endpoint 1/2/3/5, with IN buffer 64 bytes
Interrupt out endpoint 4/6, with OUT buffer 64 bytes
Support HID device sample code

3.2 SPI

SPI master mode with clock rate up to 24MHz
Data 1 bit MISO & 1 bit MOSI
SPI slave mode with clock rate up to 8MHz
Data 1 bit MISO & 1 bit MOSI
Support SPI master sample code
Support SPI slave sample code

3.3 I2C

I2C master mode support clock 100K/400K/1000K with deferent bus pull-up resistors.
100KHz with 10K ohm, 400KHz with 4.7K ohm, 1000K with 1K ohm pull up resistor.
I2C slave mode support clock 100KHz & 400KHz
Support I2C master sample code
Support I2C slave sample code

3.4 UART

Programmable baud rates <13-bit divider> with configurable oversampling ratio from 4x to 32x
Baud rate can operate asynchronous to the bus clock
Interrupt, DMA or polled operation:

- Transmit data buffer empty and transmission complete
- Receive data buffer full
- Receive overrun, parity error, framing error, and noise error

Receiver Idle detect
Receive data match
Hardware parity
Programmable 7-bit, 8-bit, 9-bit or 10-bit data mode
Programmable 1-bit or 2-bit stop bits mode
Automatic address matching
Address mark matching
Idle line address matching
Address match start/end
13-bit break character generation
11-bit break character detection
Configurable idle length detection - supporting 1, 2, 4, 8, 16, 32, 64 or 128 idle characters
FIFO depth up to 8bytes
UART TX & UART RX mode with baud rate up to 1 Mbps
Support UART TX/RX sample code

3.5 FTM (Flex Timer Module) or PWM (Pulse Width Modulation)

8 FTM (PWM) pins for output pulse width control or input pulse width detect.
Support this function on request

3.6 GPIO

8 GPIOs for GPI or GPO using, LED, switch or button.
Support GPIO control sample code

3.7 TRGMUX

The trigger multiplexer module allows software to configure the trigger source input or output for various peripherals.

3.8 Programmable CRC5-32

Support programmable CRC5 to CRC32 calculation.

4. Hardware crypto engine & functions

• Public Key Cryptography (digital signature, key agreement) › NIST standard Elliptic Curve (up to P521, B571)

› ECDSA: FIPS 186-4

› ECDH: NIST SP800-56A

› RSA: (digital signature, validation only, up to 4096) FIPS 186-4

› SM2: GM/T 0003-2012

• Private Key Cryptography › AES128/192/256: FIPS PUB 197

› SM4: GM/T 0002-2012

› ChaCha20: RFC8439

› ECB/CFB/OFB: NIST SP 800-38A

› CBC/CBC-CTS: NIST SP 800-38A

› CTR32/64/128: NIST SP 800-38A

› XTS: NIST SP 800-38E

• Secure Hash Function › SHA224/256/384/512/512_224/512_256: FIPS 180-4

› SM3: GM/T 0004-2012

• Message Authentication Code › CMAC: NIST SP 800-38B

› HMAC: FIPS 198-1

› Poly1305: RFC8439

• Authenticated Encryption › CCM/CBC-MAC: NIST SP 800-38C

› GCM/GMAC: NIST SP 800-38D

› Chacha20-Poly1305: RFC8439

• Key Wrapping › KW/KWP: NIST SP800-38F

• Key Derivation Function › KBKDF (CTR/FB): NIST SP 800-56C

› PBKDF: NIST SP 800-132

• Deterministic Random Bit Generator › CTR-DRBG (AES): NIST SP 800-90A

5. Hardware crypto engine driver

We provide SDK of hardware crypto engine drivers for partners to simplify developing their secure element product.

6. Electrical Characteristics

6.1 Absolute Maximum Ratings

Symbol	Parameter	Rating
V_{DDH}	Supply Voltage	-0.3V to 4.1V
V_{MAX}	Max Voltage on Any Pin	-0.5V to 4.1V
I_I	Digital pins Current	10 mA
I_O	Digital pins output Current	10 mA
$V_{ESD,HBM}$	ESD HBM Voltage with 1.5kΩ, 100pF (According to EIA/JESD22-A114-B)	2kV
$V_{ESD,CDM}$	ESD CDM Voltage (According to ESD Association Standard STM5.3.1 – 1999)	250V
I_{LATCH}	Latchup Immunity (According to EIA/JESD78)	100mA
T_A	Ambient Temperature	-40°C to 105°C
T_{STG}	Storage Temperature	-55°C to 125°C

- These are stress ratings only and functional operation is not implied. Exposure to absolute maximum ratings for prolonged time periods may affect device reliability.
- All voltages are with respect to ground.

6.2 Recommended Operating Conditions

Symbol	Parameter	Min	Typ	Max	Unit
VDDH	Supply voltage	3.0	3.3	3.6	V
V25	OTP voltage	2.25	2.5	2.75	V
VDD	Core voltage	1.08	1.2	1.32	V
T_A	Ambient Temperature	-40		105	°C
$T_{A,AVG}$	Average T_A over Lifetime		55		°C

- These are conditions under which the device functions but the specifications might not be guaranteed.
- For guaranteed specifications and test conditions, please see the Electrical Characteristics

6.3 Electrical Characteristics

V_{DDH}=3.3V, T_A=25°C, unless otherwise noted.

Symbol	Parameter	Test Condition	Min	Typ	Max	Unit
DC Characteristics						
I_{DDH_Active}	Current Consumption in Active Mode	USB function active mode		25		mA
$I_{DDH\_inactive}$	Inactive	For minimum inactive power, host need turn-off chip power.		1		uA
I_{DDH_VLPS}	Current Consumption in MCU VLPS	Power consumption in MCU very low power sleep mode (USB disabled)			2.5	mA
I_{DDH_VLPR}	Current Consumption in MCU VLPR	Power consumption in MCU very low power run mode (USB disabled)			3	mA
I_{DDH_Sleep}	Current Consumption in USB VLPS	Power consumption in USB very low power sleep mode (USB enabled)			2.0	mA
DC Characteristics of Digital Pins						
V_{IH}	Input Voltage High Threshold	V_{DDH} = 3.3V	0.8V_{DDH}		V_{DDH}+0.3	V
V_{IL}	Input Voltage Low Threshold	V_{DDH} = 3.3V	0		0.2V_{DDH}	V
I_{LEAK}	Input Leakage Current	0V < V_{IN} < V_{DDH}	-10		10	µA
		V_{DDH}=3.3V, -0.5V < V_{IN} < V_{DDH}+0.5V	-4.5			mA
V_{OH}	Output High Voltage	I_{OH} = 1mA	0.8V_{DDH}			V
V_{OL}	Output Low Voltage	I_{OL} = 1mA			0.1 V_{DDH}	V
C_{IN}	Pad Input Capacitance				10	pF
C_{LOAD}	Output Load Capacitance				30	pF

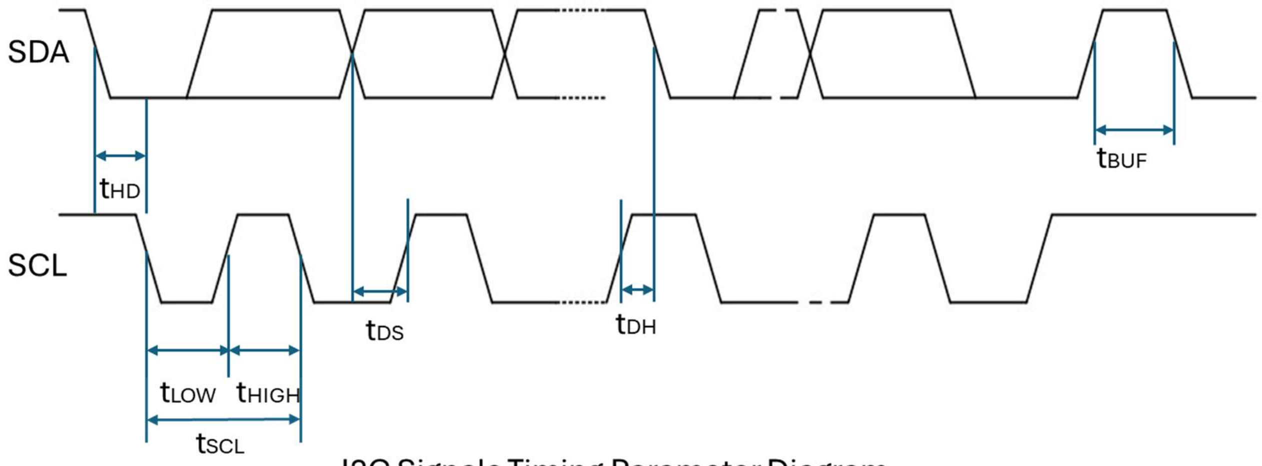
DC Characteristics of GPIO/I2C/SPI Digital pins						
V_{IH}	Input Voltage High Threshold		$0.8V_{DDH}$		$V_{DDH}+0.3$	V
V_{IL}	Input Voltage Low Threshold		0		$0.2V_{DDH}$	V
I_{LEAK}	Input Leakage Current	$0V < V_{IN} < V_{DDH},$	-10		10	µA
V_{OH}	Output High Voltage	$I_{OH} = 1mA$	$0.8V_{DDH}$			V
V_{OL}	Output Low Voltage	$I_{OL} = 1mA$			$0.1V_{DDH}$	V
$C_{O(TR)}$	Effective Output Capacitance, Time Related				10	pF
R_{PU}	PAD Pull-up Resistor		34K	51K	81K	Ω
R_{PD}	PAD Pull-down Resistor		35K	51K	84K	Ω
DC Characteristics of USB Signals (DP&DM)						
V_{DI}	Differential Input Sensitivity	DP-DM	-0.2		0.2	V
V_{CM}	Differential Common Mode Range		0.8		2.5	V
V_{FSRT}	Single Ended Receiver Threshold		0.8		2.0	V
V_{OL}	Output Low Voltage	RL=1.5K to V_{DDH}			0.3	V
V_{OH}	Output High Voltage		2.8			V
I_{LEAK}	Tri-State Data Line Leakage	$0V<Vin<V_{DDH}$	-10		10	uA
C_{LOAD}	Transceiver Capacitance				20	pF

6.4 I2C Timing Parameters

I2C Bus Timing Specification			
I2C Specification Timing Parameter	I2C Timing Symbol	I2C Timing Parameter (LPI2C functional clock cycles)	Comment
SCL clock period	tSCL	(CLKHI + CLKLO + 1 + SCL_LATENCY) x (2 ^ PRESCALE)	
Hold time Symbol Start condition	tHD	(SETHOLD +1) x (2 ^ PRESCALE)	
Low period of SCL clock	tLOW	(CLKLO + 1) x (2 ^ PRESCALE)	
High period of SCL clock	tHIGH	CLKHO x (2 ^ PRESCALE)	
Setup time Symbol Stop condition	tSU	(SETHOLD +1 + SCL_LATENCY) x (2 ^ PRESCALE)	
Data Hold Time	tDH	(DATAVLD + 1) x (2 ^ PRESCALE)	
Data Setup Time	tDS	(SDA_LATENCY+1) x (2 ^ PRESCALE)	
Bus free time between a STOP and START condition	tBUF	(CLKLO + 1 + SDA_LATENCY) x (2 ^ PRESCALE)	

# Latency time include the I/O propagation delay, the I2C Bus loading and external Pull-up resistor sizing. If Latency too large, we must slow down the I2C operation speed(tSCL).

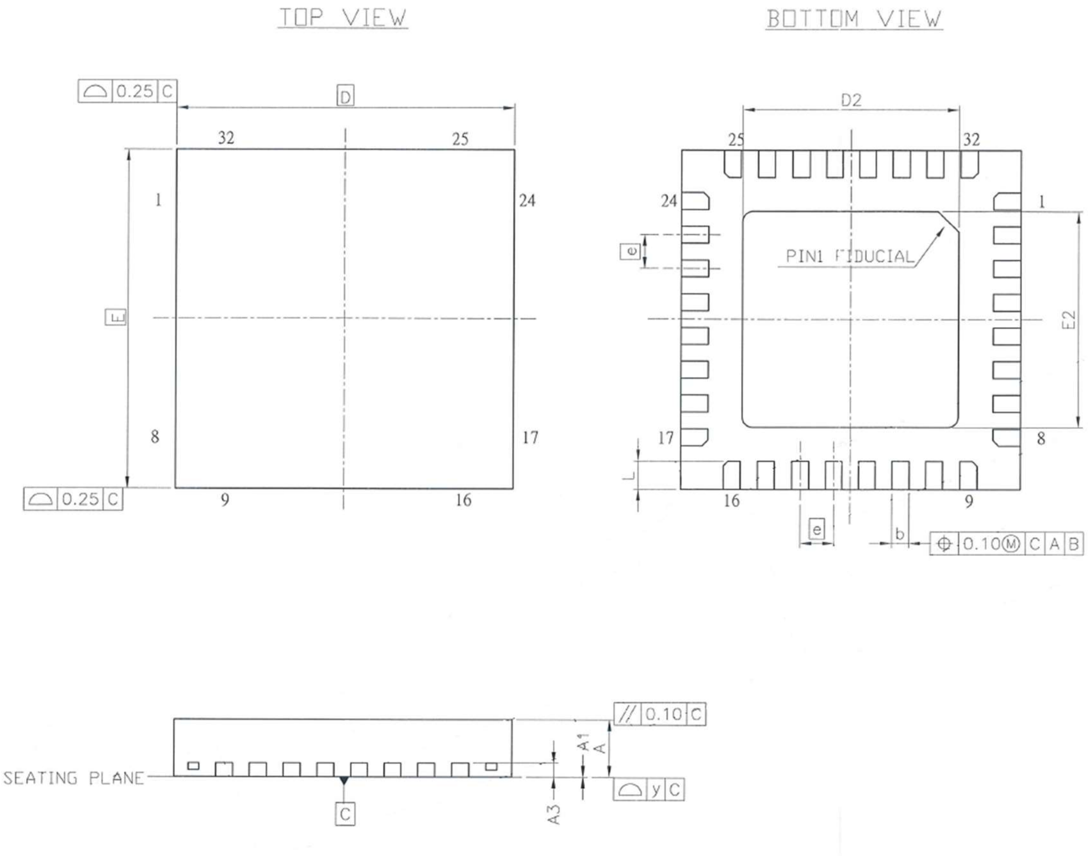
I2C Timing Parameter Restrictions Table			
I2C Timing Parameter	Minimum	Maximum	Comment
CLKLO	0x03		
CLKHI	0x03		
SETHOLD	0x02		
DATAVD	0x02	CLKLO/2 - SDA_LATENCY- 1	
FLTSCL	0x01	[CLKLO x (2 ^ PRESCALE)] - 3	
FLTSDA	FLTSCL	[CLKLO x (2 ^ PRESCALE)] - 3	
BUSIDLE	(CLKLO+SETHOLD+2) x2	CLKLO/2 - SDA_LATENCY- 1	Must also be greater than (CLKHI+1)
PRESCALE	0x0	0x7	

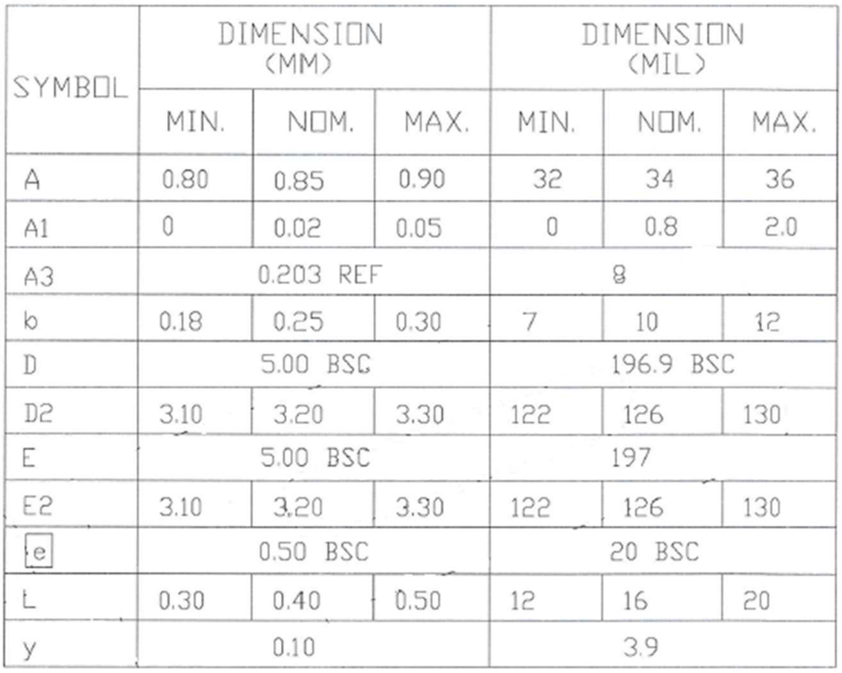


I2C Signals Timing Parameter Diagram

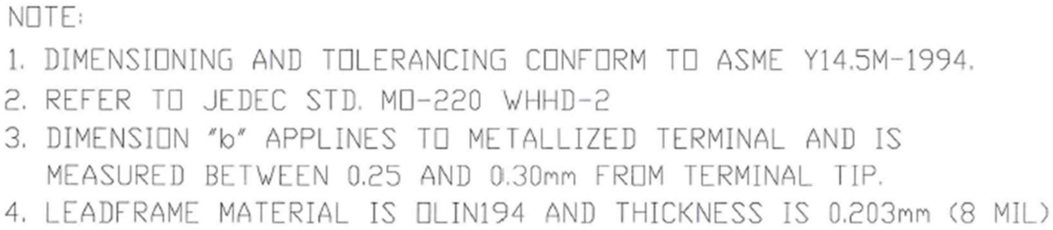
7. Package Information

CW9008 package





SYMBOL	DIMENSION (MM)			DIMENSION (MIL)		
	MIN.	NOM.	MAX.	MIN.	NOM.	MAX.
A	0.80	0.85	0.90	32	34	36
A1	0	0.02	0.05	0	0.8	2.0
A3	0.203 REF			8		
b	0.18	0.25	0.30	7	10	12
D	5.00 BSC			196.9 BSC		
D2	3.10	3.20	3.30	122	126	130
E	5.00 BSC			197		
E2	3.10	3.20	3.30	122	126	130
e	0.50 BSC			20 BSC		
L	0.30	0.40	0.50	12	16	20
y	0.10			3.9		



NOTE:

1. DIMENSIONING AND TOLERANCING CONFORM TO ASME Y14.5M-1994.
2. REFER TO JEDEC STD. MO-220 WHHD-2
3. DIMENSION "b" APPLINES TO METALLIZED TERMINAL AND IS MEASURED BETWEEN 0.25 AND 0.30mm FROM TERMINAL TIP.
4. LEADFRAME MATERIAL IS OLIN194 AND THICKNESS IS 0.203mm (8 MIL)

Abbreviation

abbreviation/notation	**meaning**
AES	Advanced Encryption Standard
AHB	Advanced High-performance Bus
AXI	Advanced eXtensible Interface
APB	Advanced Peripheral Bus
CBC	Cipher Block Chaining
CBC-CS2	CBC, Cipher Stealing option #2
CCM	Counter with CBC-MAC
CDH	Cofactor Diffie-Hellman primitive
CMAC	Cipher-based Message Authentication Code
CTR	CounTeR mode
DEK	Data Encryption Key
DMA	Direct Memory Access
DSA	Digital Signature Algorithm
EC	Elliptic Curve
ECB	Electronic Code Book
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
HMAC	Hash-based Message Authentication Code
HPC	High Performance Computing platform
ID	IDentification
KA	Key Array
KDF	Key Derivation Function
KBKDF	Key-Based Key Derivation Function
PBKDF	Password-Base Key Derivation Function
KWP	Key WraPping
MAC	Message Authentication Code
MO	block cipher Mode of Operation
NIST	National Institute of Standards and Technology
OTP	One-Time Programmable
PKC	Public Key algorithm Coprocessor
PUF	Physically Unclonable Function
SHA2	Secure Hash Algorithm, 2nd

	generation
SP	Special Publication
TRNG	True Random Number Generator
UID	Unique IDentifier

NOTICE

The specifications and product information of ChipWon Technology Co., Ltd. are subject to change without any prior notice, and customer should contact ChipWon Technology Co., Ltd. to obtain the latest relevant information before placing orders and verify that such information is current and complete.

The information provided here is believed to be reliable and accurate; however ChipWon Technology Co., Ltd. makes no guarantee for any errors that appear in this document.

LIFE SUPPORT POLICY

The products of ChipWon Technology Co., Ltd. are not designed or authorized for use as critical components in life support devices or systems without the express written approval of the president of ChipWon Technology Co., Ltd. herein:

1. Life support devices or systems are devices or systems which, (a) are intended for surgical implant into the body, or (b) support or sustain life, and (c) whose failure to perform when properly used in accordance with instructions for use provided in the labeling, can be reasonably expected to result in a significant injury of the user.
2. A critical component in any component of a life support device or system whose failure to perform can be reasonably expected to cause the failure of the life support device or system, or to affect its safety or effectiveness.