GT23SC1604

16K Bits

Secured

Serial EEPROM

Table of Contents

1. Features

- 16K serial EEPROM with security features
- Comply with ISO/IEC Standard 7816-3 Synchronous Protocol
- Store and validate security codes
- Four protected application zones
- Provide transport code security
- Single 5V power supply for read/write/erase operations
- Low power operation:
  - 15 µA (max.) standby current
  - 3 mA (max.) read current at 300 KHz
  - 4 mA (max.) write/erase current
- 2 ms read access time at 300 KHz; 5 ms write cycle time
- 300 KHz serial clock rate
- High ESD protection: > 4 KV
- High reliability:
  - 1,000,000 erase/write cycles
  - 10 years data retention
- Standard CMOS Process
- Wide operating temperature range
  - 0°C to +70°C Commercial
  - –40°C to +85°C Industrial
- Data access only after validation of security code
- Permanent invalidation of device upon eight consecutive failed attempts to enter the correct security code
- Separate read/write/erase access protections for each application zone
- Allow the memory chip to be personalized if the internal security fuse is not blown. If the internal security fuse is blown, maximum security protection of the memory will always be enabled.

2. General Description

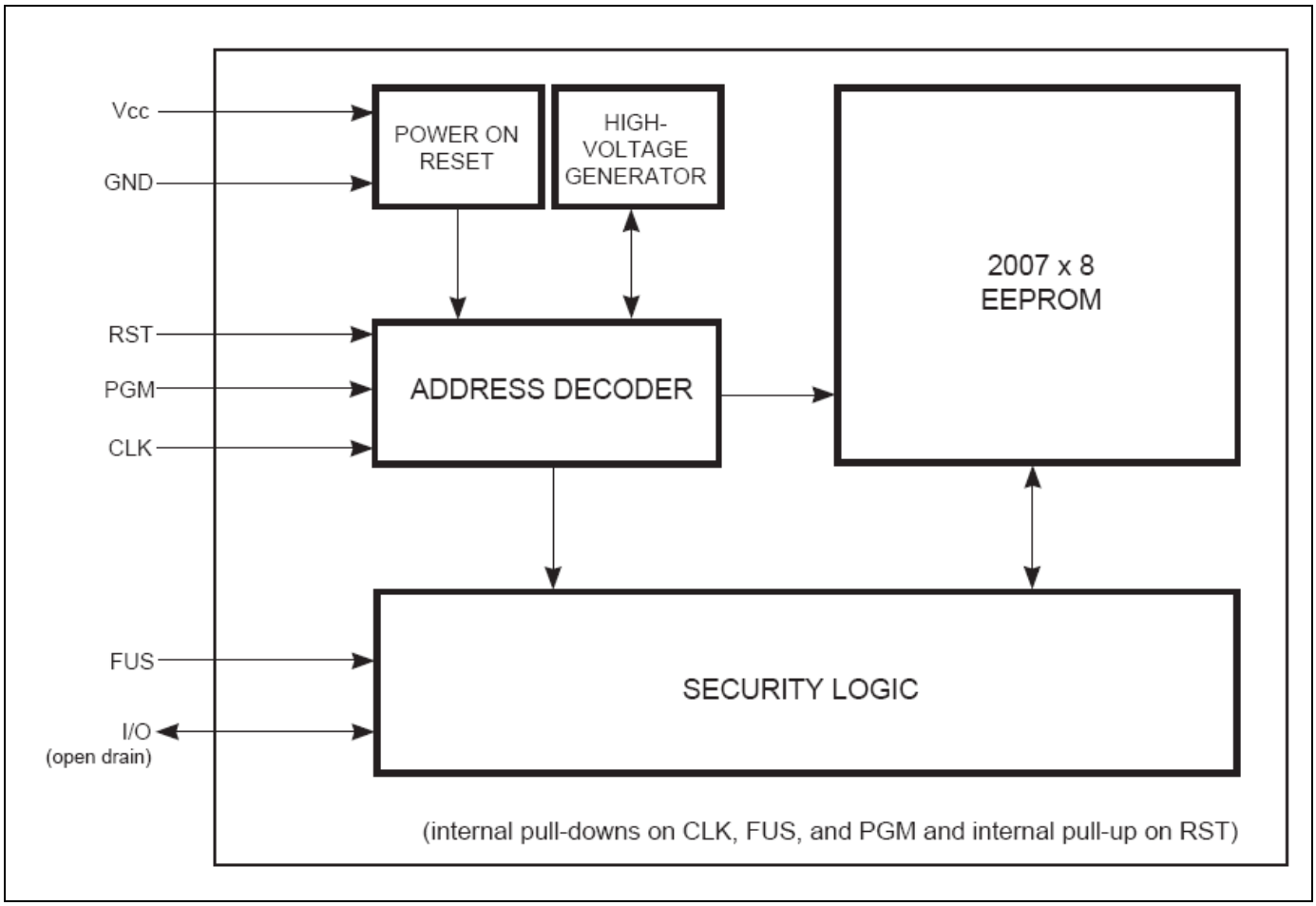
GT23SC1604 is a low-cost, low-power, highly secured 16K bits (2K x 8) serial EEPROM. It is fabricated using Giantec's advanced CMOS technology.

The security features of GT23SC1604 provide high levels of memory security protection for smart card applications.

The memory is partitioned into four application zones. Each individual application zone is protected by multiple security codes from unauthorized read/write/erase access to the zone. In addition, an internal security fuse is available for the card issuer to fully personalize the device before releasing it to customer.

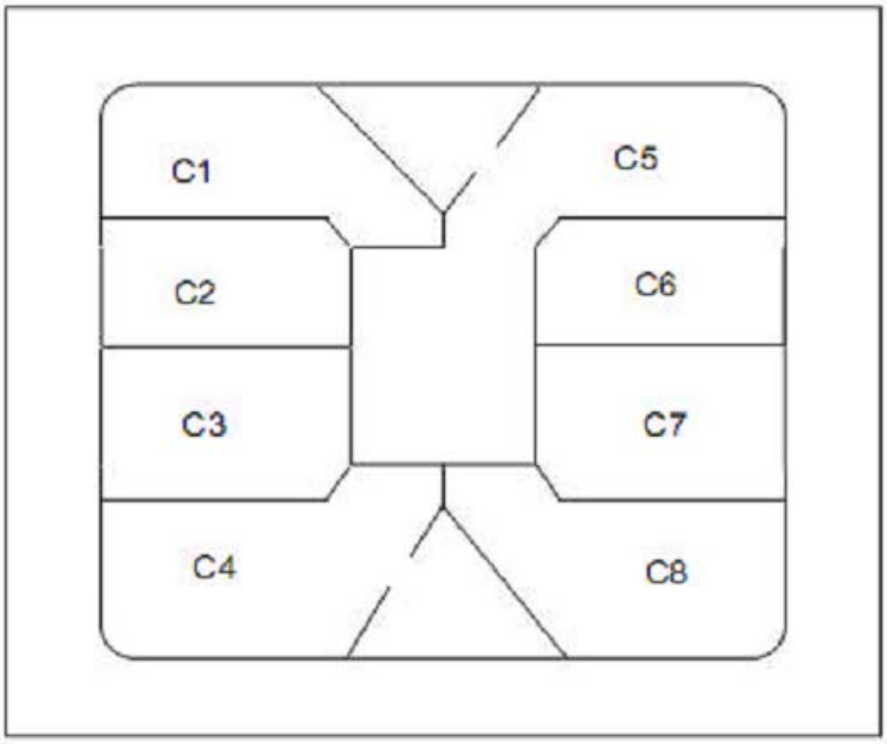
The device also features an internal high-voltage charge pump for memory programming, 1,000,000 write/erase cycles and ten years of data retention.

3. Functional Block Diagram



4. Pin Configuration

4.1 8-Pin Module (Top View)



4.2 Pin Definition

ISO	PAD	Pin Name	Definition
C1	8	V_{CC}	Supply Voltage
C2	7	RST	Reset
C3	6	CLK	Serial Clock and Address Control
C4	5	FUS	Security Fuse Pad
C5	4	GND	Ground
C6	3	NC	No Connect
C7	2	I/O	Bi-directional Data
C8	1	PGM	Programming Control

Note:

1. Pins CLK, FUS, and PGM have internal pull-downs. Pin RST has an internal pull-up.

4.3 Pin Descriptions

Symbol	Card Contact	Name and Function
V_{CC}	C1	Supply Voltage
RST	C2	Reset: The device's RST pin can be used to clear the internal address counter. When CLK is LOW, a HIGH-to-LOW transition on RST resets the address counter to zero, and the first bit of memory will be output on I/O after the falling edge of RST. Also, the RST pin can be used to place the device in low power standby mode by placing RST in HIGH logic state and both PGM and FUS in LOW logic state. While RST is HIGH, the internal address counter will not be incremented with CLK.
CLK	C3	Serial Clock and Address Control: This is the device data clock pin. It is used to clock data bits into and out of the device. It also increments the internal address counter.
FUS	C4	Security Fuse Pad: This pin is used by card issuer to personalize the device before releasing it to the customer. When FUS pin is driven to logic HIGH state and the state of the internal security fuse is HIGH (not blown), the issuer can personalize the entire content of the memory with successful Security Code (SC) validation. When FUS pin is driven to logic LOW state and the state of the internal security fuse is HIGH (not blown), the full protection of the memory is enabled and the security features of the device can be tested by the issuer. After the device personalization is completed, the issuer should blow the internal security fuse to logic LOW state so that the full protection of the memory will always be enabled regardless of the state on FUS pin. (Refer to GT23SC1604 Security Levels and also Blowing Internal Security Fuse.)
GND	C5	Ground
NC	C6	No Connect
I/O	C7	Serial Data Input and Output: This pin is where the data bit is shifted in and out of the device when a clock pulse is applied to CLK pin.
PGM	C8	Programming Control: This pin is asserted HIGH to initiate memory write or erase operation.

5. GT23SC1604 Operation

5.1 Power-On Reset (POR)

When the supply voltage is first applied to the device, the device initiates POR. All the internal flags are clear (refer to Definition of GT23SC1604 Internal Flags), and the internal address counter is reset to zero.

5.2 Reset

With CLK LOW, a HIGH-to-LOW transition at RST resets the address counter to zero. After the falling edge of RST, the device outputs the first bit of the memory on I/O pin. The reset operation will have no effect on any internal flags (see AC Test Load).

5.3 Addressing

Addressing is handled by an internal address counter which is incremented on the falling edge of CLK. When the counter continues to increment past 16383, the counter will roll over back to zero. The counter can also be cleared to zero by the reset operation.

5.4 Read

If read access to a memory bit is enabled, the state of the bit can be read out of the device by incrementing the address counter to the bit location. The device outputs the state of the read bit on the I/O pin after the falling edge of the last clock pulse that increments the address counter to the read bit location. However, if the read access to the memory bit is inhibited, the state of the data bit will not be output and the I/O pin will be placed in high-impedance state '1' (see Reset Timing Diagram).

5.5 Compare

Compare operation allows users to input the security/erase key code for the security/erase key code validation for read/write/erase access to protected application zones (refer to Security/Erase Key Code Validation Operation).

The compare operation latches the user's input Security/Erase Key bit into the device at the rising edge of CLK and the bit comparison is performed on the next falling edge of CLK. The compare and read operations are executed in the same manner. The device distinguishes between the two operations by testing the address counter for security/erase key code location and the state of corresponding security/erase key code valid comparison flag (see Read Timing Diagram).

5.6 Write

If write access to a memory bit is enabled, the content of the bit can be written over with a '0' value by performing the following sequence: select PGM (logic HIGH state), input '0' on the I/O pin, change CLK from LOW- to-HIGH, deselect PGM (logic LOW state), wait for 5 ms programming delay, and then bring CLK down from HIGH-to-LOW to complete the write operation. The new state of the bit will be output at the end of the write operation after the falling edge of CLK for data verification (see Compare Timing Diagram).

5.7 Erase

If erase access to a memory bit is enabled, the content of the bit can be written over with a '1' value with the erase operation. Although erase is performed on single bits, the erase operation writes FFH to the whole byte which contains the erased bits because the memory is organized into 8-bit bytes. The erase operation can be executed by performing the following sequence: select PGM (logic HIGH state), input '1' on the I/O pin, change CLK from LOW-to-HIGH, deselect PGM (logic LOW state), wait for 5 msec programming delay, and then bring CLK down from HIGH-to-LOW to complete the erase operation. The new state of the bit will be output at the end of the erase operation after the falling edge of CLK for data verification (see Compare Timing Diagram).

5.8. Device Operation(1)

Operation	FUS	PGM	RST	CLK	Definition
Reset	X	X		0	The address counter is reset to zero and the first bit of the memory is output after the falling edge of RST.
INC/Read	X	0	0		The address counter is incremented and the first bit is output after the falling edge of the clock if read access to the bit location is enabled.
INC/CMP	X	0	0		Compare the input bit with the internal bit of the memory (for Security/Erase Key codes validation). The address counter is incremented on the falling edge of CLK. The input bit is latched into the device at the rising edge of CLK and the bit comparison is done on the next falling edge of CLK.
Erase/Write	X	1	0		For write operation (write a '0' to the current address), a '0' is placed on I/O before the rising edge of CLK. For erase byte operation (write FFH to the byte that contains the current bit), a '1' is placed on I/O before the rising edge of CLK. CLK must stay HIGH for 5 ms during memory programming.
Verify	X	0	0		The new content of the current address will be output after the falling edge of CLK for verification.
Standby	0	0	1	X	The device is placed into standby mode. In this mode, the address counter will not be incremented with clock pulse when RST is HIGH.

Note:

1. X = Don't Care.

6. Electrical Characteristics

6.1 Absolute Maximum Ratings

Symbol	Parameter	Value	Unit
V_{CC}	Supply Voltage	-0.3 to + 6	V
V_I/V_O	Input/Output Voltage	–0.3 to +6	V
T_{STG}	Storage Temperature	–40 to +125	°C
P_{max}	Power Dissipation	60	mV

Note: Stress greater than those listed under Absolute Maximum Ratings may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other condition outside those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect reliability.

6.2 Operating Range

Range	Ambient Temperature (T_A)	V_{CC}
Commercial	0°C to +70°C	5V
Industrial	–40°C to +85°C	5V

6.3 Capacitance [1, 2]

Symbol	Parameter	Conditions	Max.	Unit
CIN	Input Capacitance	V_{IN} = 0V	5	pF
COUT	Output Capacitance	V_{OUT} = 0V	8	pF

Notes: [1] Tested initially and after any design or process changes that may affect these parameters and not 100% tested.

[2] Test conditions: T_A = 25°C, f = 1 MHz, V_{CC} = 5.0V+10%; GND=0.

6.4 DC Electrical Characteristic [1]

Industrial: T_A = –40°C to +85°C, V_{CC} = 1.8V ~ 5.5V

Symbol	Parameter	Test Conditions	Min.	Typ.	Max.	Unit
V_{CC}	Supply Voltage		4.5	5. 0	5.5	V
V_{IH}	Input High Level		2		V_{CC}+0.3	V
V_{IL}	Input Low Level		-0.3		0.8	V
I_{LI}	Input Leakage Current				50	μA
I_{LH}	I/O Leakage Current	V_{OH} = 5V Open Drain			50	μA
V_{OL}	Output Low Level	I_{OL} = 1 mA	—		0.4	V
I_{CC}	Supply Read/Compare Current	TA=25°C, F_{CLK}=300KHz	—		3.0	mA
I_{CCP}	Supply Write/Erase Current	TA=25°C	—		4.0	mA
I_{CCSB}	Standby Supply Current	TA=25°C, RST=5V; FUS, CLK, PGM=0V, I_{IO}=0mA	—		15	μA

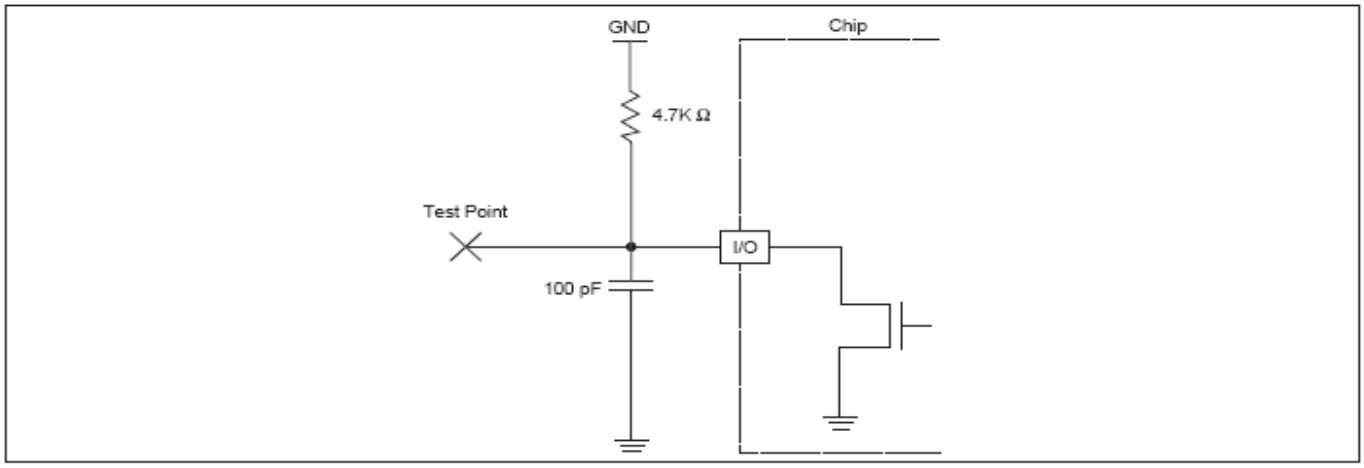
Notes: [1] There is a internal pull-up on pin RST. There are internal pull-downs on pins FUS, CLK and PGM

6.5 AC Electrical Characteristic

AC Test Conditions

Parameter	Value
Input Pulse Levels	GND to 3.0V
Input Rise and Fall Time	5ns
Input and Output Timing and Reference Level	0.8V and 2.0V
Output Load	100pF

AC Test Load

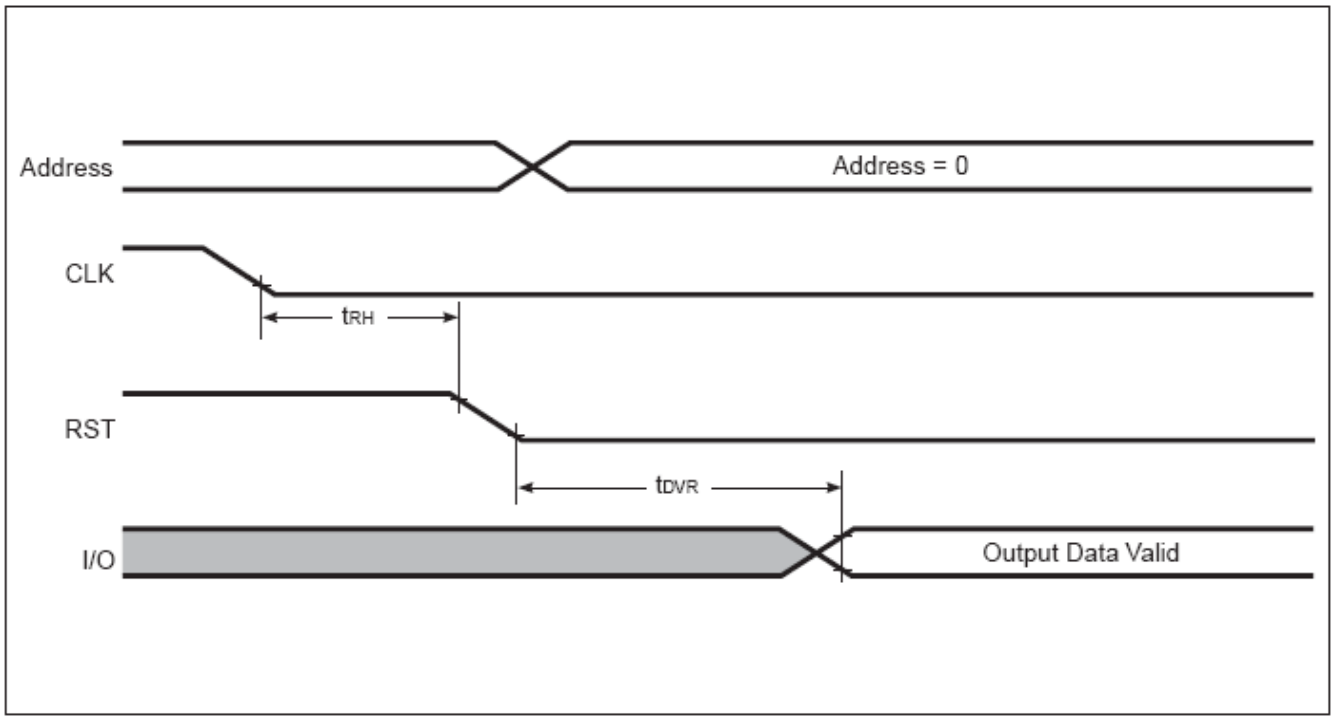


AC Electrical Characteristics (TA = 0 to 70°C, Vcc = 5.0V + 10%; GND = 0V)

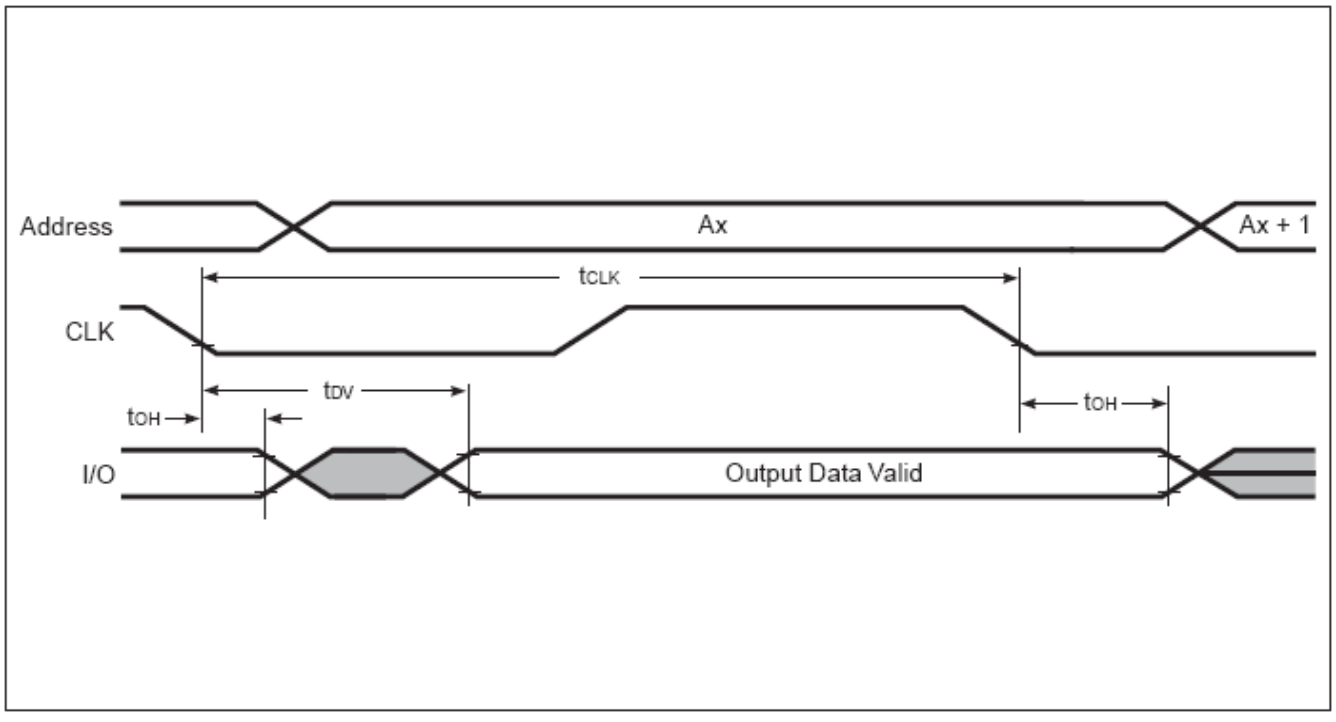
Symbol	Parameter[1]	Min.	Typ.	Max	Unit
F_{CLK}	Clock Frequency	—	—	300	KHz
T_{CLK}	Clock Cycle Time	3.3	—	—	ms
T_{RH}	RST Hold Time	0.1	—	—	ms
T_{DVR}	Data Valid Reset to Address 0	—	—	2.0	ms
T_{CH}	CLK Pulse Width (High)	0.2	—	—	ms
T_{CL}	CLK Pulse Width (Low)	0.2	—	—	ms
T_{DV}	Data Access	—	—	2.0	ms
T_{OH}	Data Hold	0	—	—	ms
T_{SC}	Data in Setup (CMP Instruction)	0	—	—	ms
T_{HC}	Data in Hold (CMP Instruction)	0.2	—	—	ms
T_{CHP}	CLK Pulse Width (High in Erase/Write)	5	—	—	ms
T_{DS}	Data in Setup	0.2	—	—	ms
T_{DH}	Data in Hold	0	—	—	ms
T_{SPR}	PGM Setup	2.2	—	—	ms
T_{HPR}	PGM Hold	0.2	—	—	ms

7. Diagram

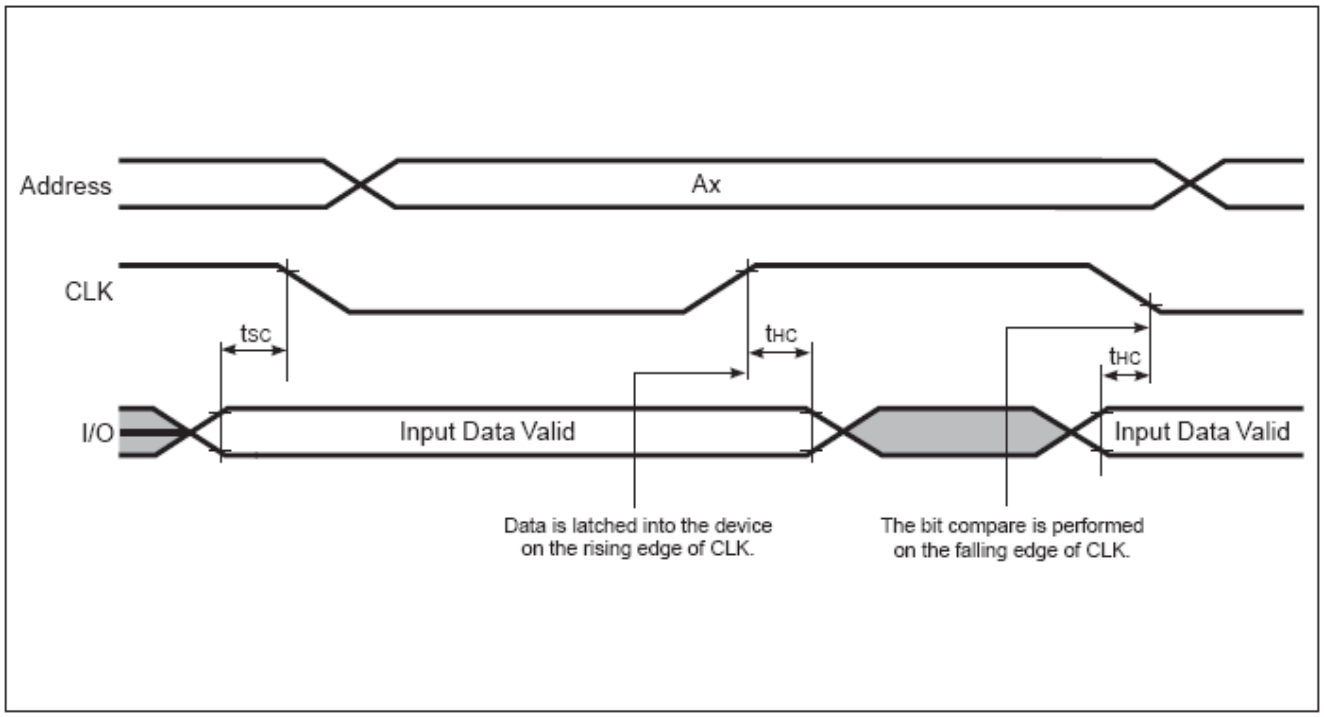
Reset Timing Diagram



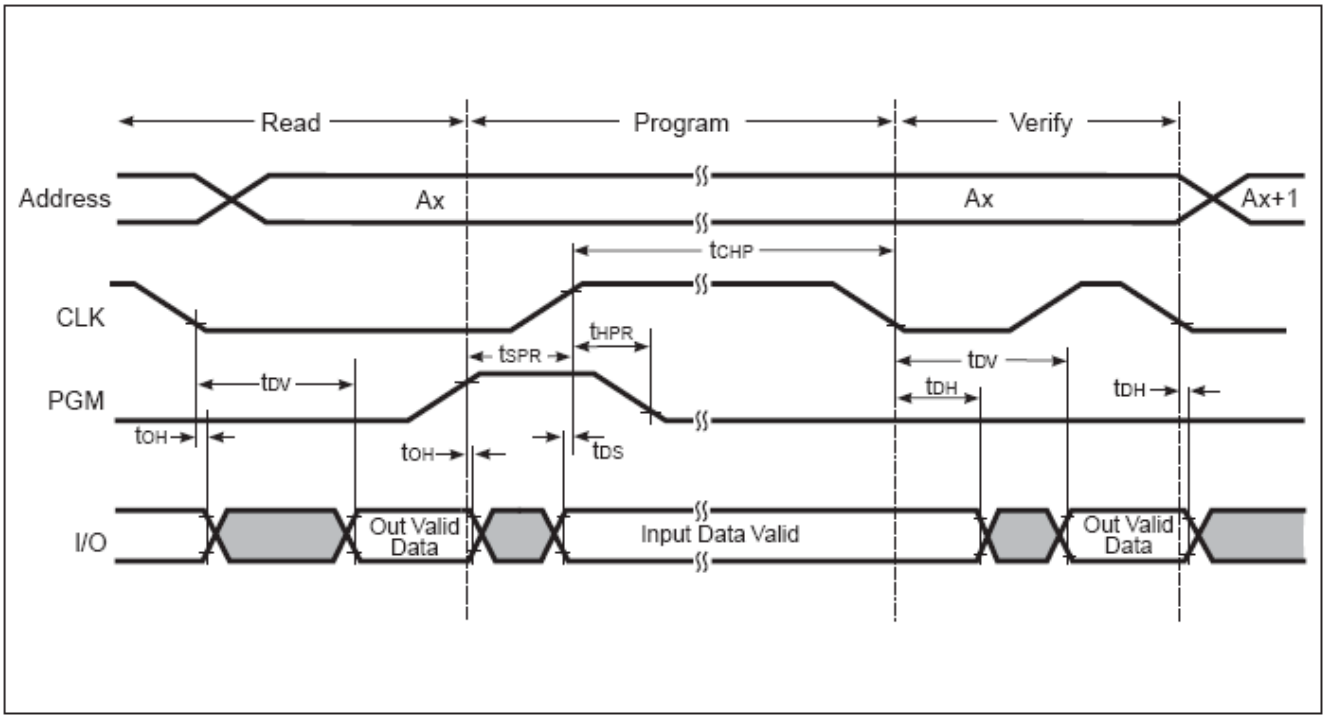
Read Timing Diagram



Compare Timing Diagram



Write/Erase Timing Diagram



8. GT23SC1604 MEMORY MAP

GT23SC1604 memory is divided into four Application Zones. Each Application Zone has a corresponding access security code, access attempts counter (only Application Zone 1), erase key, erase attempts counter, and data storage area. Below is the memory map table for GT23SC1604:

Memory Map

Symbol	Description	Start Bit Address	End Bit Address	Bits	Start Byte Address	End Byte Address	Bytes
FZ	Fabrication Zone	0	15	16	0	1	2
IZ	Issuer Zone	16	79	64	2	9	8
SC	Security Code	80	95	16	10	11	2
SCAC	Security Code Attempts Counter	96	103	8	12	12	1
CPZ	Code Protected Zone	104	167	64	13	20	8
Application 1							
SC1	Application Zone 1 Security Code	168	183	16	21	22	2
S1AC	Application Zone 1 SC1 Attempts Counter	184	191	8	23	23	1
EZ1	Application Zone 1 Erase Key	192	207	16	24	25	2
E1AC	Application Zone 1 EZ1 Attempts Counter	208	215	8	26	26	1
AZ1	Application Zone 1	216	9775	9560	27	1221	1195
Application 2							
SC2	Application Zone 2 Security Code	9776	9791	16	1222	1223	2
EZ2	Application Zone 2 Erase Key	9792	9807	16	1224	1225	2
E2AC	Application Zone 2 EZ2 Attempts Counter	9808	9815	8	1226	1226	1
AZ2	Application Zone 2	9816	11863	2048	1227	1482	256
Application 3							
SC3	Application Zone 3 Security Code	11864	11879	16	1483	1484	2
EZ3	Application Zone 3 Erase Key	11880	11895	16	1485	1486	2
E3AC	Application Zone 3 EZ3 Attempts Counter	11896	11903	8	1487	1487	1
AZ3	Application Zone 3	11904	13951	2048	1488	1743	256
Application 4							
SC4	Application Zone 4 Security Code	13952	13967	16	1744	1745	2
EZ4	Application Zone 4 Erase Key	13968	13983	16	1746	1747	2
E4AC	Application Zone 4 EZ4 Attempts Counter	13984	13991	8	1748	1748	1
AZ4	Application Zone 4	13992	16039	2048	1749	2004	256
MTZ	Memory Test Zone	16040	16055	16	2005	2006	2
Total Addressable EEPROM Memory				16056			2007
Fuse	Internal Security Fuse	16288	16303				
	Last Bit Address		16383				

9. GT23SC1604 MEMORY PARTITIONS

Fabrication Zone (FZ)

This zone is programmed by the manufacturer. After the zone is programmed, the manufacturer disables the write/erase access to this zone so that it cannot be changed by card issuer or card user.

Issuer Zone (IZ)

This zone can only be programmed by the issuer during device personalization process.

Security Code (SC)

This code serves as master security password to access to device's memory. A special transport code is programmed into SC location by the manufacturer and it is only made known to the issuer. This special code secures the transport of the device between the manufacturer and the issuer. After the issuer successfully validates the transport code, SC can be freely altered as wished. After the internal security fuse is blown, SC protects the access to the four application zones of the device.

Security Code Attempts Counter (SCAC)

Counts number of failed attempts to input the correct Security Code (SC) to the device. After eight consecutive failed attempts, the device will be locked permanently.

Code Protected Zone (CPZ)

This zone is read access only. Access to erase or write to this zone is protected by Security Code (SC).

Application Zone Security Codes (SC1, SC2, SC3, SC4)

These codes protect access to individual application zones of the memory.

Application Zone Security Code Attempts Counter (S1AC)

Counts number of failed attempts to input the correct Application Zone 1 Security Code to the device. After eight consecutive failed attempts, the Application Zone 1 will be locked permanently.

Application Zone Erase Keys (EZ1, EZ2, EZ3, EZ4)

These keys protect individual application zones (AZ1, AZ2, AZ3, AZ4) from unauthorized attempt to erase the zone.

Application Zone Erase Keys Attempts Counter (E1AC, E2AC, E3AC, E4AC)

Counts number of failed attempts to input the correct application zone erase key to the device. After eight consecutive failed attempts, the erasure of the corresponding application zone will never be allowed (refer to Memory Access Table).

Application Zones (AZ1, AZ2, AZ3, AZ4)

Each application zone provides protected data storage space for user application. The read, write and erase access to the application zone are controlled by the first two bits of the zone as well as the corresponding application zone security code and application zone erase key and the Security Code (refer to Memory Access Table).

Memory Test Zone (MTZ)

There are no protections on this zone.

9.1 GT23SC1604 SECURITY LEVELS

There are two security levels available in GT23SC1604 which are controlled by the internal security fuse state and FUS pin. At security level 1, the issuer has access to the entire memory with successful Security Code (SC) validation and the issuer is allowed to personalize the content of the entire memory except the Fabrication Zone (FZ). At security level 2, the memory is fully protected by various security codes in the memory. When the card has been personalized, the internal security fuse should be blown to protect the card memory from unauthorized usage before the card is released to the customer (Refer to Blowing Internal Security Fuse). Once the security fuse is blown, it cannot be changed again. Below is the truth table that shows how the security level can be set with the state of FUS input pin.

Security Levels

FUS pin	State of the Internal FUSE	Security Level
GND	Don't Care	2
Vcc	HIGH (FUSE not blown)	1
Vcc	LOW (FUSE blown)	2

9.2 GT23SC1604 INTERNAL FLAGS

The GT23SC1604's internal flags enable/disable the read, write, and erase access to application zones (Refer to Memory Access Table). All the flags are clear upon power-on reset (POR). The flags can be set to logic '1' state by validating the corresponding security code through the validation process. Once the flag is enabled ('1' state), it cannot be cleared by any operations except POR.

Security Code Valid Comparison Flag (SV)

This flag is set to '1' after the Security Code (SC) is validated (see Security/Erase Key Code Validation). This flag protects an unpersonalized card from unauthorized usage. If the card has already been personalized, this flag provides master protection for the application zones (refer to Memory Access Table).

Application Zone 1 Security Code Valid Comparison Flag (S1)

This flag is set to '1' after the Application Zone 1 Security Code (SC1) is validated (see Security/Erase Key Code Validation). This flag provides access protection for Application Zone 1 (refer to Memory Access Table).

Application Zone 'm' Security Code Valid Comparison Flag (Sm) where 'm' = 2, 3 or 4.

This flag is set to '1' after the Application Zone 'm' Security Code is validated (see Security/Erase Key Code Validation). This flag provides access protection for Application Zone 'm' (refer to Memory Access Table).

Application Zone 'n' Erase Key Valid Comparison Flag (Sn) where 'n' = 1, 2, 3 or 4.

This flag is set to '1' after the Application Zone 'n' Erase Key is validated (see Write/Erase Timing Diagram). This flag provides protection for Application Zone 'n' from unauthorized erasure of the zone (refer to Memory Access Table).

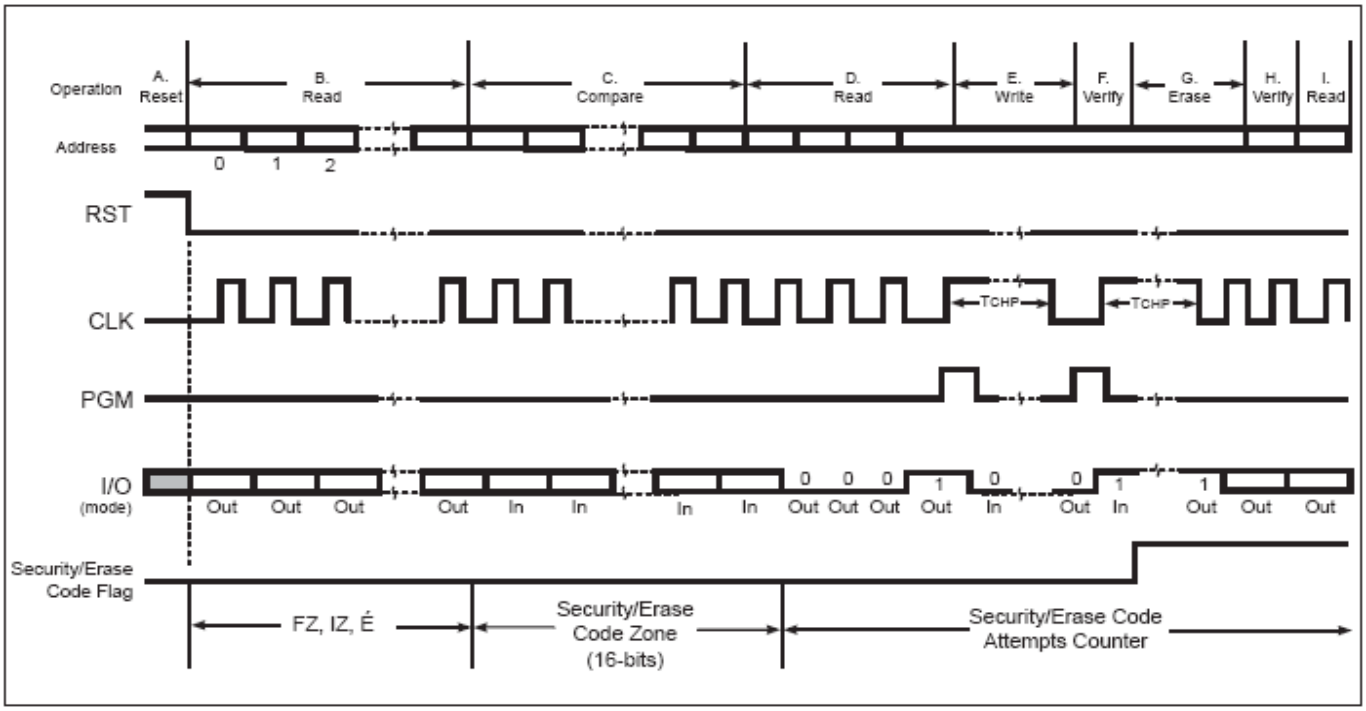
Application Zone 'n' write flag (Pn) where 'n' = 1, 2, 3 or 4.

This flag is set to '1' if the first bit of Application Zone 'n' is '1' (Bit address: 216 for zone 1, 9816 for zone 2, 11904 for zone 3, or 13992 for zone 4). This flag enables write access to the corresponding application zone (refer to Memory Access Table).

Application Zone 'n' read flag (Rn) where 'n' = 1, 2, 3 or 4.

This flag is set to '1' when the second bit of Application Zone 'n' is '1' (Bit address: 217 for zone 1, 9817 for zone 2, 11905 for zone 3, or 13993 for zone 4). This flag enables read access to the corresponding application zone (refer to Memory Access Table).

Security/Erase Key Code Validation



9.3 SECURITY/ERASE KEY CODE VALIDATION OPERATION (For SC, SC1, EZ1, EZ2, EZ3, and EZ4 validation)

A. Reset the address counter to zero.

B. Send required number of clock pulses to increment the address counter to security/erase key code location.

C. Input the security/erase key code bit by bit for code validation.

D. After security/erase key code entry, look for the first logic '1' bit in security/erase key code attempts counter. If the '1' bit is found, do not increment the address.

E. Write a '0' over the '1' bit in security/erase key code attempts counter at the current bit location.

F. The chip outputs a '0' after programming is done.

G. If the security/erase key code validation was successful, the corresponding comparison flag will be set to '1' on the rising edge of PGM and the security/erase key code attempts counter should be erased to reactivate the eight allowable attempts. (The validation operation can be aborted by setting CLK HIGH when PGM is still LOW.)

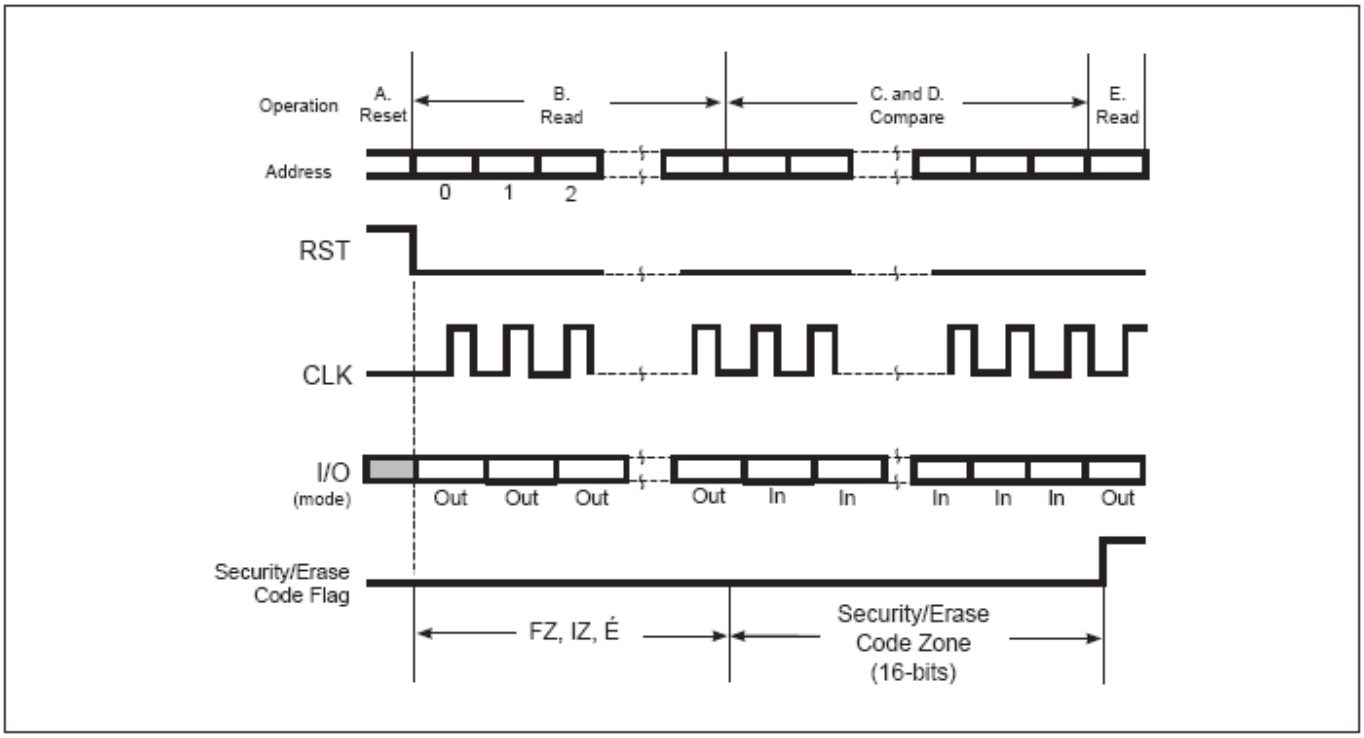
H. If the comparison flag were successfully set to '1', the erasure of the attempt counter would be allowed and the device would output a '1' on I/O after the erase operation. Otherwise, the erasure of the attempt counter would be blocked and a '0' would be output on I/O. (The content of the attempt counter remains unchanged.)

I. On the following edge of the clock, the address counter is incremented and the state of the next bit is output on I/O.

Notes:

1. The address counter does not increment from steps E to H
2. After eight consecutive failed attempts to validate the security/erase key code, the corresponding flag will be locked at '0' permanently.

Application Zone Security Code Validation



9.4 APPLICATION ZONE SECURITY CODE VALIDATION OPERATION (For SC2, SC3, and SC4 validation)

A. Reset the address counter to zero.

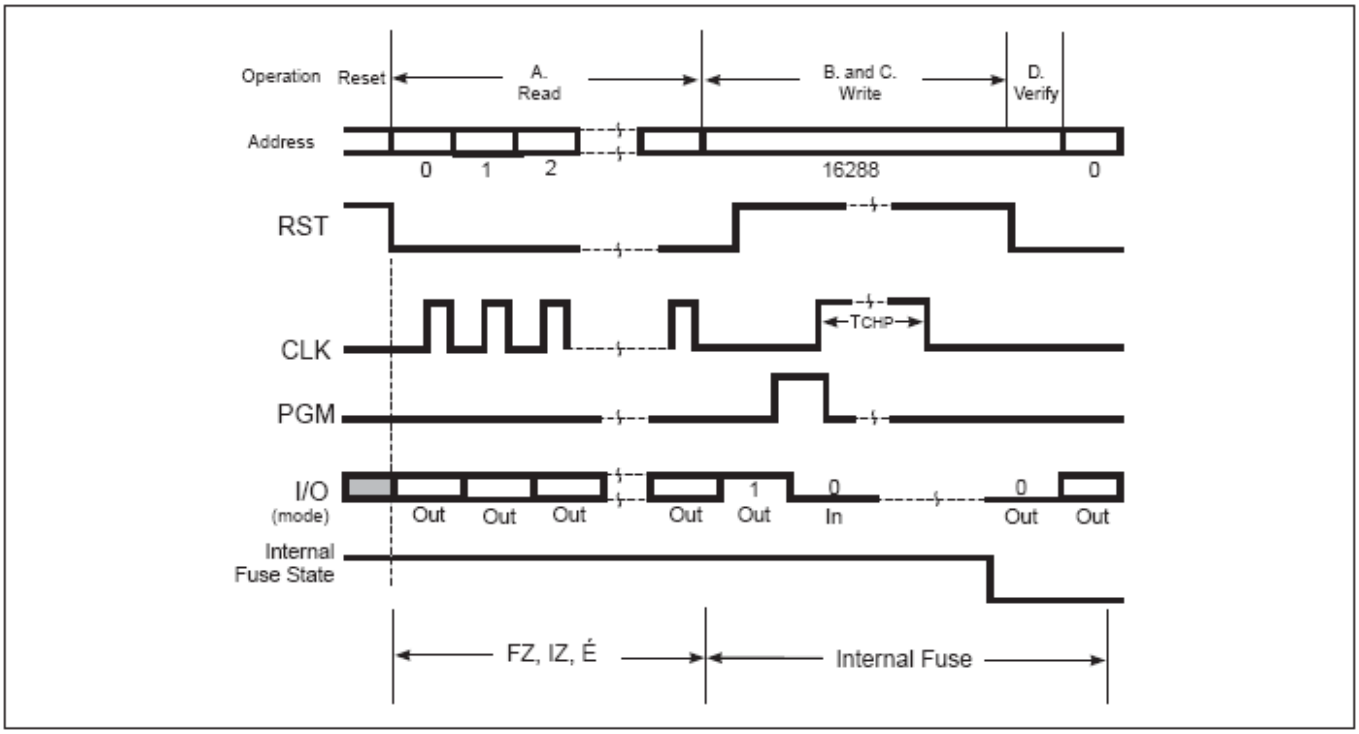
B. Send required number of clock pulses to increment the address counter to application zone security code location.

C. Input the application zone security code bit by bit for code validation.

D. If the security code validation were successful, the corresponding comparison flag would be set to '1'.

E. On the following edge of the clock, the address counter is incremented and the state of the next bit is output on I/O.

Blowing Internal Security Fuse



9.5 BLOWING INTERNAL SECURITY FUSE

A. Set the address counter between 16288 and 16303.

B. Set FUS pin at Vcc or GND; set RST pin at Vcc.

C. Write '0' to the current bit location.

D. The chip outputs a '0' after programming is done. The state of the internal security fuse is now '0' (blown state).

Note:

1. SV flag must be enabled (HIGH state) to blow the internal security fuse.

9.6 MEMORY ACCESS TABLE

9.6.1 Security Level One

At security level one (security fuse not blown and FUS pad at Vcc), the memory access is controlled by Security Code Valid Comparison Flag (SV) and Application Zone 'n' read flag (Rn).

Memory Access Conditions At Security Level 1 (Device Personalization)

Fields	SV	Rn	Read	Erase (Write '1')	Write (Write '0')	Compare
FZ	X	X	Yes	No	No	No
IZ	0	X	Yes	No	No	No
	1	X	Yes	Yes	Yes	No
SC	0	X	No	No	No	Yes
	1	X	Yes	Yes	Yes	No
SCAC	0	X	Yes	No	Yes	No
	1	X	Yes	Yes	Yes	No
CPZ	0	X	Yes	No	No	No
	1	X	Yes	Yes	Yes	No
SCn	0	X	No	No	No	No
	1	X	Yes	Yes	Yes	No
S1AC	0	X	Yes	No	No	No
	1	X	Yes	Yes	Yes	No
EZn	0	X	No	No	No	No
	1	X	Yes	Yes	Yes	No
EnAC	0	X	Yes	No	No	No
	1	X	Yes	Yes	Yes	No
AZn	0	0	No	No	No	No
	0	1	Yes	No	No	No
	1	X	Yes	Yes	Yes	No
MTZ	X	X	Yes	Yes	Yes	No

Note:
1. 'n' corresponds to Application Zone 'n' where 'n' = 1, 2, 3, or 4.

9.6.2 Security Level Two

At security level two (security fuse blown or FUS pad at GND), memory access is controlled by SV, Sn, Pn, Rn and En flags.

Memory Access Conditions At Security Level 2 (Product Release)

Fields	SV	Sn	Pn	Rn	En	Read	Erase (Write '1')	Write (Write '0')	Compare
FZ	X	X	X	X	X	Yes	No	No	No
IZ	X	X	X	X	X	Yes	No	No	No
SC	0	X	X	X	X	No	No	No	Yes
	1	X	X	X	X	No	Yes	Yes	No
SCAC	0	X	X	X	X	Yes	No	Yes	No
	1	X	X	X	X	Yes	Yes	Yes	No
CPZ	0	X	X	X	X	Yes	No	No	No
	1	X	X	X	X	Yes	Yes	Yes	No
SCn	0	X	X	X	X	No	No	No	No
	1	0	X	X	X	No	No	No	Yes
	1	1	X	X	X	No	Yes	Yes	No
S1AC	0	X	X	X	X	Yes	No	No	No
	1	0	X	X	X	Yes	No	Yes	No
	1	1	X	X	X	Yes	Yes	Yes	No
EZn	0	X	X	X	X	No	No	No	No
	1	0	X	X	0	No	No	No	No
	1	1	X	X	0	No	No	No	Yes
	1	1	X	X	1	No	Yes	Yes	No
EnAC	0	X	X	X	X	Yes	No	No	No
	1	0	X	X	0	Yes	No	No	No
	1	1	X	X	0	Yes	No	Yes	No
	1	1	X	X	1	Yes	Yes	Yes	No
AZn	X	0	X	0	X	No	No	No	No
	X	0	X	1	X	Yes	No	No	No
	1	1	0	X	0	Yes	No	No	No
	1	1	0	X	1	Yes	Yes	No	No
	1	1	1	X	0	Yes	No	Yes	No
	1	1	1	X	1	Yes	Yes	Yes	No
MTZ	X	X	X	X	X	Yes	Yes	Yes	No

Note:
1. 'n' corresponds to Application Zone 'n' where 'n' = 1, 2, 3, or 4.

10. Ordering Information

Order Part Number	Package
GT23SC1604-X07MB005-TR	8-PIN Module

11. Revision History

Revision	Date	Descriptions
A0	Jan. 2010	Initial version