EPROM Programming

1.1. Internal ROM Features

The internal ROM of the TSC80251G1 derivatives contains five different areas:

- Code Memory
- Configuration Bytes
- Lock Bits
- Encryption Array
- Signature Bytes

1.1.1. EPROM/OTP Devices

All the Internal ROM but the Signature Bytes of the TSC87251G1 products is made of EPROM cells. The Signature Bytes of the TSC87251G1 products are made of Mask ROM.

The TSC87251G1 products are programmed and verified in the same manner as Intel's 87C251Sx, using the same algorithm, which programs at VPP=12.75V using a series of five 100 µs pulses per bytes. This results in a programming time of approximately 16 seconds for the 16 Kbyte on–chip code memory.

The EPROM of TSC87251G1 products in Window CQPJ is erasable by Ultra–Violet radiation (UV). UV erasure set all the EPROM memory cells to one and allows a reprogramming. The quartz window must be covered with an opaque label when the device is in operation. This is not so much to protect the EPROM array from inadvertent erasure, as to protect the RAM and other on–chip logic. Allowing light to impinge on the silicon die during device operation may cause a logical malfunction.

Note:
Erasure of the EPROM begins to occur when the chip is exposed to light wavelength shorter than 4000Å. Since sunlight and fluorescent light have wavelength in this range, exposure to these light sources over an extended time (1 week in sunlight or 3 years in room–level fluorescent lighting) could cause inadvertent erasure.

The TSC87251G1 products in plastic packages are One Time Programmable (OTP). Then an EPROM cell cannot be reset by UV once programmed to zero.

1.1.2. Mask ROM Devices

All the Internal ROM of TSC83251G1 products is made of Mask ROM cells. They can be verified using the same algorithm as the EPROM/OTP devices.

1.1.3. ROMless Devices

The TSC80251G1 products include only Configuration Bytes and Signature Bytes made of Mask ROM cells. They can be verified using the same algorithm as the EPROM/OTP devices.

These products do not include on–chip Code Memory, Lock Bits or Encryption Array.

1.1.4. Security Features

In some microcontrollers applications, it is desirable that the user program code be secured from unauthorized access. The TSC87251G1 and TSC83251G1 products offer two kinds of protection for program code stored in the on–chip array:

- Program code in the on–chip Code Memory is encrypted when read out for verification if the Encryption Array is Programmed.
- A three–level lock bit system restricts external access to the on–chip code memory.

1.1.5. Lock Bit System

The TSC87251G1 derivatives implement 3 levels of security for User's program as described in Table 1.

The first level locks the programming of the User's internal Code Memory and the Encryption Array. The Configuration Bytes and the Lock Bits are always programmable.

The second level locks the verifying of the User's internal Code Memory. It is always possible to verify the Configuration Bytes and the Lock Bits. It is never possible to verify the Encryption Array.

The third level locks the external execution.

Table 1 **Lock bits programming**

Level	Lock bits LB[2:0]	Internal Execution	External Execution	Verify	Programmable	External PROM read (MOVC)
0	000	Yes	Yes	Yes*	Yes	Yes**
1	001	Yes	Yes	Yes*	No	No
2	011	Yes	Yes	No	No	No
3	111	Yes	No	No	No	No
Reserved	Other	x	x	x	x	x

Notes:
** returns encrypted data if Encryption Array is programmed.*
*** returns non encrypted data.*

Level 1 should be set before programming Level 2; Level 2 should be set before programming Level 3.

The security level may be verified according to Table 2.

Table 2 **Lock bits verification**

Level	Lock bits Data
0	xxxxx000
1	xxxxx001
2	xxxxx01x
3	xxxxx1xx

1.1.6. Encryption Array

The TSC87251G1 and TSC83251G1 controllers include a 128–byte Encryption Array located in nonvolatile memory outside the memory address space. During verification of the on–chip code memory, the seven low–order address bits also address the Encryption Array. As the byte of the code memory is read, it is exclusive–NOR'ed (XNOR) with the key byte from the Encryption Array. If the Encryption Array is not programmed (still all 1s), the user program code is placed on the data bus in its original, unencrypted form. If the Encryption Array is programmed with key bytes, the user program code is encrypted and cannot be used without knowledge of the key byte sequence.

To preserve the secrecy of the encryption key byte sequence, the Encryption Array can not be verified.

Caution:
When a MOVC instruction is executed the content of the ROM is not encrypted. In order to fully protect the user program code, the lock bit level 1 (see Table 1) must always be set when encryption is used.

Note:
The TSC83251G1 derivatives do not provide lock bit choice. However they always provide the protection of the lock bit level 1 (see Table 1) when the encryption is used.

Caution:
If the encryption feature is implemented, the portion of the on–chip code memory that does not contain program code should be filled with "random" byte values other than FFh to prevent the encryption key sequence from being revealed.

1.2. Signature Bytes

The TSC87251G1, TSC83251G1 and TSC80251G1 contain factory–programmed Signature Bytes. These bytes are located in non–volatile memory outside the memory address space at 30h, 31h, 60h and 61h. To read the Signature Bytes, perform the procedure described in section 1.4., "Verify Algorithm", using the verify signature mode (see Table 5). Signature byte values are listed in Table 3.

Table 3 **Signature Bytes (Electronic ID)**

		Signature Address	Signature Data
Vendor	TEMIC	30h	58h
Architecture	C251	31h	40h
Memory	16K ROM	60h	FBh
Revision	None (Intel core step A) First (Intel core step D)	61h	FFh FEh

1.3. Programming Algorithm

Figure 1 shows the hardware setup needed to program the TSC87251G1 EPROM areas:

- The chip has to be put under reset and maintained in this state until the completion of the programming sequence.
- Then PSEN# has to be to forced to a low level for 14 clock cycles before any other operation and it has to be maintained in this state until the completion of the programming sequence.
- The voltage on the EA# pin must be set to VCC.
- The programming mode is selected according to the code applied on Port 0. It has to be applied until the completion of this programming operation.
- The programming address is applied on Ports 1 and 3 which are respectively the Most Significant Byte (MSB) and the Least Significant Byte (LSB) of the address.
- The programming data are applied on Port 2.

- The EPROM Programming is done by raising the voltage on the EA# pin to VPP, then by generating low level pulses on ALE/PROG# pin (See Table 4).
- The voltage on the EA# pin must be lowered to VCC before completing the programming operation.
- It is possible to alternate programming and verification operation (See section 1.4.). Please make sure the voltage on the EA# pin has actually been lowered to VCC before performing the verification operation.

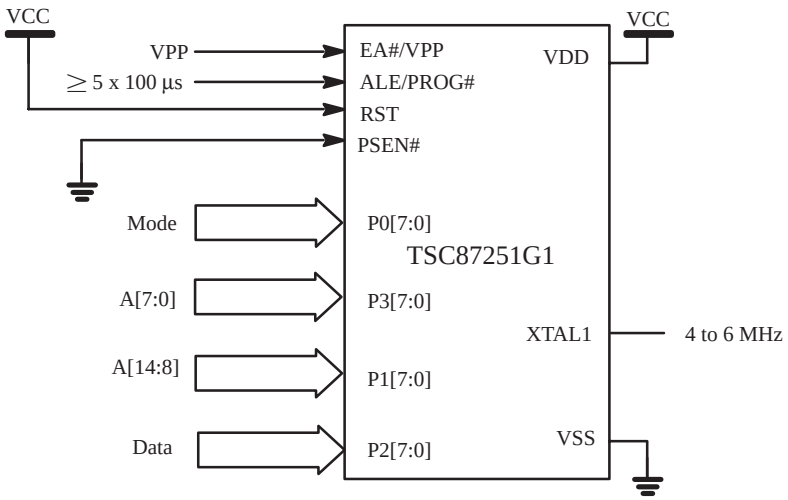

Figure 1 **Setup for EPROM Programming**

Table 4 **EPROM Programming Modes**

EPROM Mode	RST	EA#	PSEN#	ALE/PROG#	P0	P2	P1(MSB) P3(LSB)	Notes
On–chip Code Memory	1	VPP	0	≥ 5 Pulses	68h	Data	Address (16K) 0000h-3FFFh	1
Configuration Bytes	1	VPP	0	≥ 5 Pulses	69h	Data	CONFIG0: 0080h CONFIG1: 0081h	1
Lock Bits	1	VPP	0	≥ 5 Pulses	6Bh	X	LB0: 0001h LB1: 0002h LB2: 0003h	1
Encryption Array	1	VPP	0	≥ 5 Pulses	6Ch	Data	0000h-007Fh	1

Notes:
1. The ALE/PROG# pulse waveform is shown in Figure 3.

1.4. Verify Algorithm

Figure 2 shows the hardware setup needed to verify the internal ROM areas of the TSC80251G1 derivatives:

- The chip has to be put under reset and maintained in this state until the completion of the verify sequence.
- Then PSEN# has to be to forced to a low level for 14 clock cycles before any other operation and it has to be maintained in this state until the completion of the programming sequence.
- The voltage on the EA# pin must be set to VCC and ALE must be set to an high level.
- The Verify Mode is selected according to the code applied on Port 0. It has to be applied until the completion of this verification.
- The verification address is applied on Ports 1 and 3 which are respectively the MSB and the LSB of the address.
- Then device is driving the data on Port 2. It is valid 48 clock periods after the address is stable.
- It is possible to alternate programming and verification operation (See section 1.3.). Please make sure the voltage on the EA# pin has actually been lowered to VCC before performing the verification operation.

Table 5 **Verify Modes**

Verify EPROM	RST	EA#	PSEN#	ALE	P0	P2	P1(MSB) P3(LSB)
On–chip code memory	1	1	0	1	28h	Data	Address (16K) 0000h-3FFFh
Configuration Bytes	1	1	0	1	29h	Data	0080h-0083h
Lock Bits	1	1	0	1	2Bh	Data	0000h
Signature Bytes	1	1	0	1	29h	Data	30h, 31h, 60h, 61h

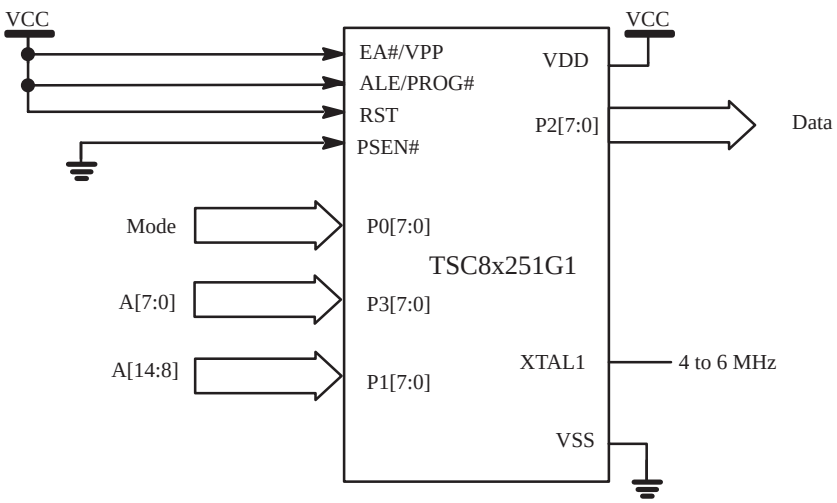

Figure 2 **Setup for Verification**

1.5. AC Characteristics

Table 6 **EPROM Programming & Verification Characteristics**
(TA = 0 to 40°C ; VCC = 5V ± 10%)

Symbol	Parameter	Min	Max	Units
VPP	Programming Supply Voltage	12,5	13	V
IPP	Programming Supply Current		75	mA
T_{OSC}	Oscillator Frequency	167	250	ns
T_{AVGL}	Address Setup to PROG# low	$48T_{OSC}$		
T_{GHAX}	Address Hold after PROG# low	$48T_{OSC}$		
T_{DVGL}	Data Setup to PROG# low	$48T_{OSC}$		
T_{GHDX}	Data Hold after PROG#	$48T_{OSC}$		
T_{EHSH}	ENABLE High to VPP	$48T_{OSC}$		
T_{SHGL}	VPP Setup to PROG# low	10		µs
T_{GHSL}	VPP Hold after PROG#	10		µs
T_{GLGH}	PROG# Width	90	110	µs
T_{AVQV}	Address to Data Valid		$48T_{OSC}$	
T_{ELQV}	ENABLE low to Data Valid		$48T_{OSC}$	
T_{EHQZ}	Data Float after ENABLE	0	$48T_{OSC}$	
T_{GHGL}	PROG high to PROG# low	10		µs

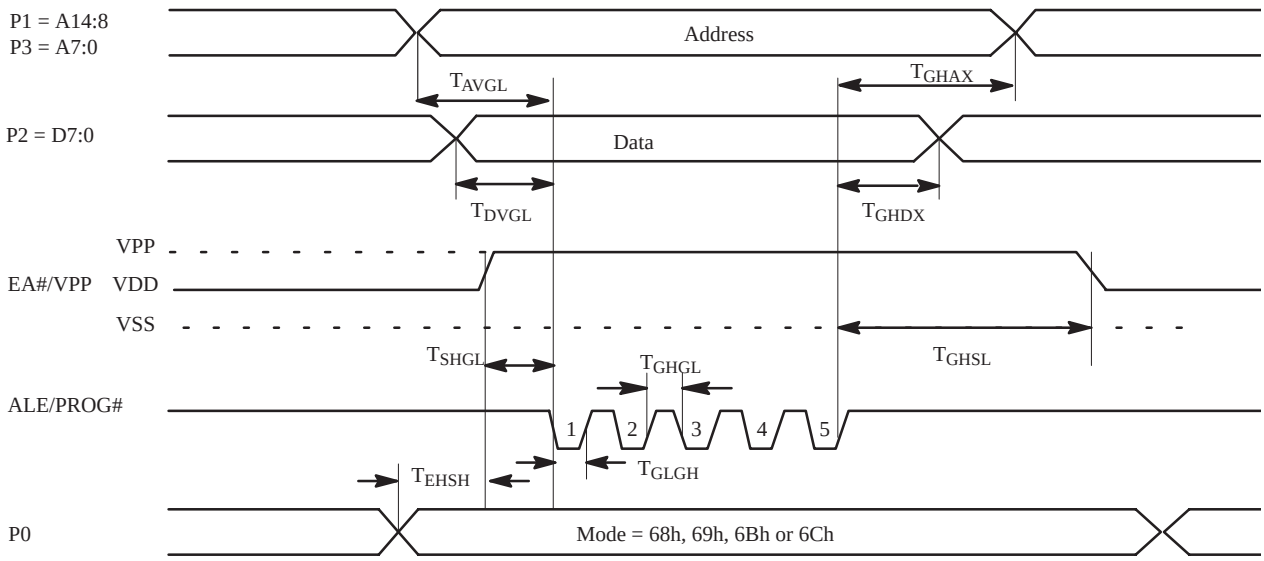

Figure 3 **Timings for EPROM Programming**

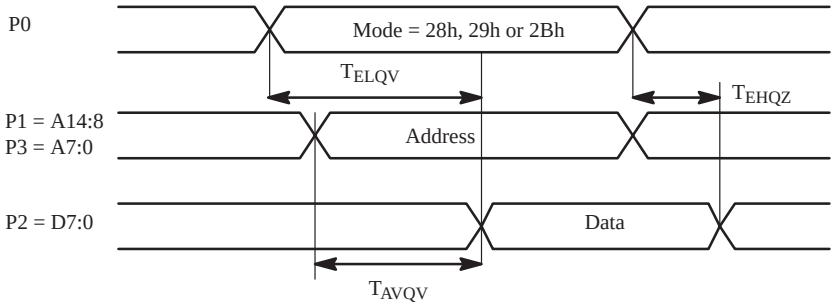

Figure 4 **Timings for EPROM Verification**