Encryption on 80C51 Family Microcontrollers

Introduction

MHS provides a hardware encryption mechanism in order to protect the program memory against piracy.
For this purpose, an encryption array is scrambled within the ROM matrix.

This array is programmed by the factory at the same time as the program memory, its content being different for each application, and is totally secure from outside.
The size of the encryption array depends on the size of the ROM matrix :

- 128 bytes for 80C51
- 256 bytes for 80C52
- 512 bytes for 83C154
- 1024 bytes for 83C154D

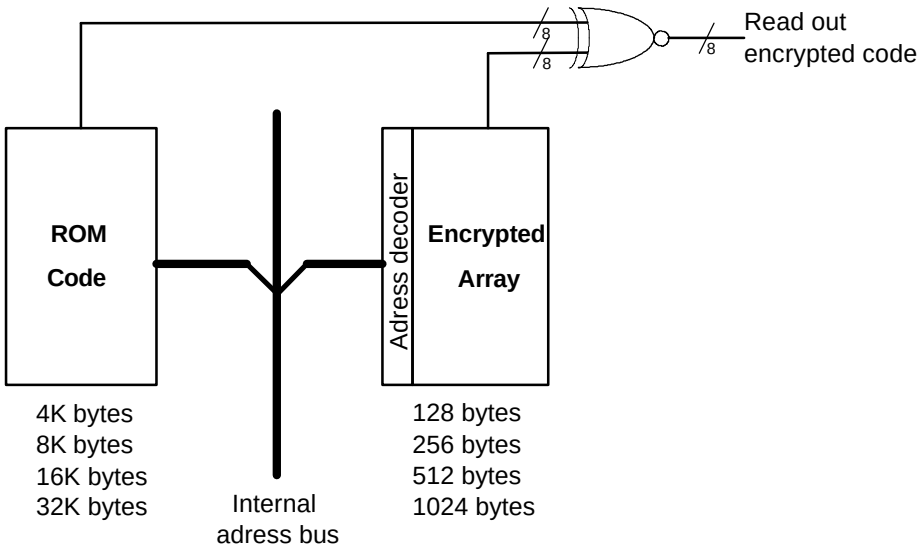
When the internal code is read out at a given address, this address selects one byte of the ROM memory map and one byte of the encrypted array following an algorithm.
These two bytes are combined to create an encrypted byte at the output port.

Design Considerations

When the program verification is performed, or when MOVC instructions are executed from external memory for accessing internal memory, each byte of internal ROM is exclusive-nor'ed with an encryption byte, in order to provide on Port 0 an encrypted byte.

The algorithm for selecting one encryption byte uses a combinaison of the internal memory address lines :

- 7 address lines for 80C51
- 8 address lines for 80C52
- 9 address lines for 83C154
- 10 address lines for 83C154D



Adding Features

The External Access pin (EA) is sampled and latched on RESET, and any further switching of this pin is not recognized.

It is always possible to use external memory, but the state of EA during RESET will ascertain what is enabled.

- EA = 0
  - Code memory is exclusively external
  - MOVC instructions access external ROM and return non encrypted data.
- EA = 1
  - Code memory is internal for the lower 4K, and external for the upper bytes for 80C51 (limit is 8K for 80C52, 16K for 83C154 and 32K for 83C154D).
  - MOVC instructions in external ROM code that access internal ROM return encrypted data.

This ensures full protection of ROM content, as detailed in the table below :

Table 1. Use of MOVC intruction to access data in ROM code.

EA	Program counter *	Data pointer *	Program memory	Data	Comments
1	< 4K	< 4K	Internal	Internal	Internal fetches during internal MOVC instruction : data not encrypted
1	< 4K	> 4K	Internal	External	External fetches during internal MOVC instruction : data not encrypted
1	> 4K	< 4K	External	Internal	Internal fetches during external MOVC instruction : data encrypted
1	> 4K	> 4K	External	External	External fetches during external MOVC instruction : data not encrypted
0	X	X	External	External	External fetches during external MOVC instructions : data not encrypted

* : 4K value is for 80C51. Replace by 8K for 80C52, by 16K for 83C154D and by 32K for 83C154D

Additional Information

For additional information on Microcontrollers, and Ordering Information, please refer to the following datasheets available upon request :

- 80C31/80C51
- 80C32/80C52
- 80C154/83C154
- 83C154D