Enhancing System Security with Macronix Flash

Introduction

Protecting system operation from intentional tampering or fatal unrecoverable errors is of critical importance in many applications. Systems need to be protected against software or hardware tampering in order to safeguard sensitive data, protect intellectual property, protect digital rights or prevent unauthorized use. Malicious software attacks may also cause disruption of services and result in customer dissatisfaction and a loss of revenue. This technical note describes the main threats related to the memory system and Macronix Flash memory security features that can be used to enhance system security.

Overview of System Security Needs

Attacks on a system typically alter or copy the content of the Flash image for three primary reasons, which are to:

i. operate the system in an unauthorized manner with the purpose of committing fraud against the user or service provider.
ii. disrupt the functionality of many systems through a denial of service.
iii. reverse-engineer the system in order to clone its data/code or to exploit its security weaknesses.

To achieve the above goals, both hardware and software skills are needed. The attack may come from direct tampering of a single system or from software spread through viruses in connected devices. The systems that more frequently have to deal with security are those connected to payment/billing services such as Set-Top Box, mobile devices (such as smart phones) and metering devices.

Standard Macronix flash memory products already include some basic protection features such as Write/Erase Block Protection, a One Time Programmable (OTP) area and/or a Unique Identifier. More advanced security features such as Read Protection and Permanent Block Locking are also offered in the Macronix secure product lines.

Some of the possible attack types, countermeasures, and secure memory features are shown in Table 1.

Table 1. Attacks and Countermeasures

Attack Type	Threats / Purpose	Countermeasure	Secure Memory Features
Replace System Memory	-Unauthorized system use -Fraud	Memory Identity Check at system boot time	-Unique ID -OTP Area -Secret Key Authentication
Modify Software Parameters or Code	-Unauthorized system use -Fraud	Check code validity at boot time using hash-type digest verification	-OTP Area -Block Protection
		Store the code in protected memory	Block Protection
Capture “on-line” Bus Activity	-Cloning or System modification -Reverse engineering -Fraud	Protect Bus lines from probing	BGA package
Capture Data Code “offline” after removing (de-soldering) the flash	-Cloning or System modification -Fraud	Read Protection	Read Protection

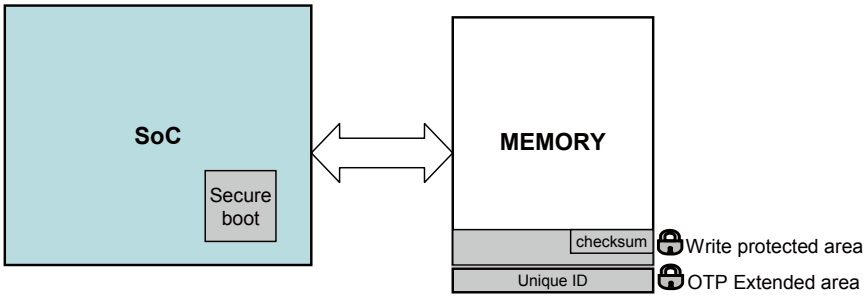
From a system security standpoint, it is absolutely necessary to protect the system during the initial boot stage. System checks at the boot stage are of fundamental importance to ensure that the system has not been altered and can work properly. The boot stage might also be able to restore the system to a known safe state in the case when a system check is failing. A “secure boot” is sometimes supported by chipsets having specific secure hardware features, however in many cases, the boot procedures rely solely on the code stored in the external memory. This is the most critical situation, where proper memory security features can provide the most benefit to enhance security.

"Figure 1. Boot Checks Procedures" shows a system where a secure boot first stage is run internally from the System on Chip (SoC). The Figure also shows that the memory might be provided with Unique ID, serial number, and write protected areas that might be used during the boot process described below.

At boot time the SoC checks all the security critical components in the system to verify their integrity. With respect to the memory system there are two fundamental checks to be performed:

i. check the authenticity of all external memory components.
ii. check the authenticity of the memory content (software and parameters).

Figure 1. Boot Checks Procedures



If checks performed at boot time fail regarding the corruption or authenticity of the code, a procedure to operate in a safe mode may be implemented. In some cases the system might be able to completely restore the software independently, without the need of (human) service intervention.

Check of Component Authenticity

Checking the authenticity of a memory component to make sure it has not been swapped with an unauthorized one can be done by employing Macronix memory components. A unique ID number programmed at the factory may be used for such purpose. The unique ID is usually stored in the extended One Time Programmable (OTP) area of NOR Flash memories. To access such additional memory space it is necessary to use a specific command. In NAND memories, the Unique ID can be retrieved using Read ID commands. The microcontroller can compare the read-out of the ID with the original one stored in a safe area. The main security loophole in this verification scheme is when the memory has been swapped with a counterfeit component with the ID cloned.

Check of Code Authenticity

A second security check, usually performed at the boot stage, concerns the verification of the integrity or authenticity of the memory code. This is usually done by calculating a hash-type digest of the memory content that can be compared to a reference value stored safely. A checksum value can be stored inside the microcontroller if it has this capability or it could be stored inside the external memory in the One Time Programmable (OTP) Area or in Sectors that can be locked permanently.

The signature value is usually calculated by hash-type algorithms such as SHA-x or other proprietary methods. The method chosen should have a low probability of collision. For example SHA-256 is considered secure but other methods with lower computation effort can also be adopted depending on the application. Unique ID and Code verification yield the best security if both are implemented in the system.

For more advanced authentication implementations, memory products may make use of secret key based algorithms. For this type of advanced requirements, please contact Macronix.

Write Protection

To avoid unintentional or intentional modifications to system memory - especially the section storing security critical parameters such as the verification digest number – sectors can be write-protected. Many write protection mechanisms are available and they are based on either simple software lock/unlock commands, or password enabled lock/unlock commands or even permanent lock commands.

The simple software lock/unlock commands could be used by the system at boot time in order to lock the system during operation. This protection can ensure that the memory is not altered unintentionally. A hardware protection method, based on whether a Write Protect (WP#) pin is tied physically to ground or not, is also usually available to prevent the protection from being disabled by unauthorized software.

In addition, password lock mechanisms can reasonably guarantee that no hacker can unlock a sector unless the password is compromised in some way.

Using a Permanent lock feature is an extreme protection mechanism to prevent anyone from ever changing the memory content once it is activated

To learn more about which Macronix Flash Memory Protection mechanisms are available in which Macronix product families, please refer to the following section “Security Features available in Macronix Products”.

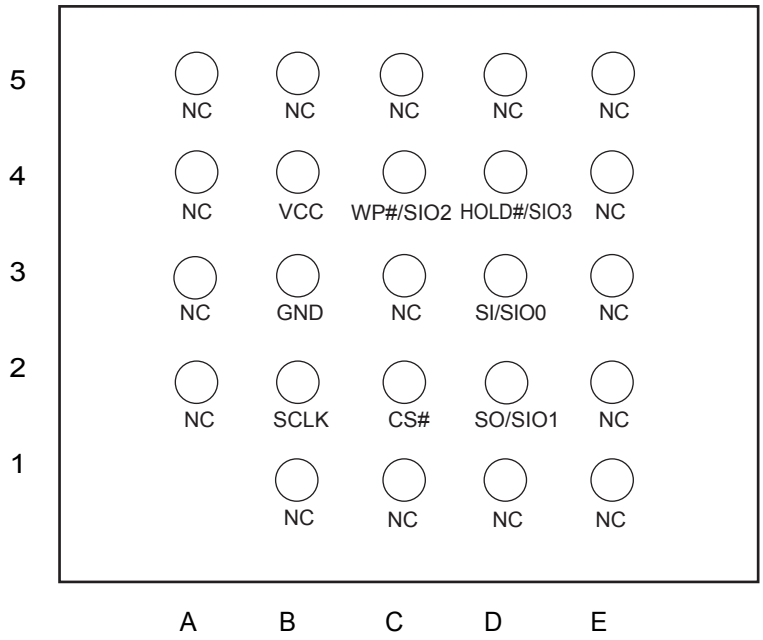
Proprietary Code Protection

Piracy attacks might also aim at retrieving security sensitive system information or stealing proprietary code and algorithms. Different level of protection can be applied in order to protect the systems against such kinds of attack.

First, the system can be assembled in such a way that the data and control signal lines between the microcontroller and the memory are not easily accessible from tracing their values or voltage levels. Proper PCB layout and Ball Grid Array packages that do not expose the pinout of the chips are often used to achieve the protection.

Macronix offers products with standard BGA packages. The secure package consists of a Ball Grid Array (BGA) package with a proper pinout as shown in *"Figure 2. Secure BGA Pinout"*. The inner pins are connected to the memory while the external corona acts as a barrier for probing while the memory is plugged onto the board.

Figure 2. Secure BGA Pinout



However, a hacker with superior capability could de-solder the part and expose the memory pins. A system solution that combines the memory die (KGD) inside the same package of the SoC could further enhance the security as all the connections are hidden inside the package.
Another layer of protection could be added by encrypting the code stored in the memory so that its content cannot be deciphered by hackers. The decryption process must be done internally within the microcontroller however this might not be possible for performance reasons in many cases.
Read protection might also be used to provide additional security for proprietary code. A Read protection scheme can be implemented using Macronix Secure products. With such secure memory products it is necessary to provide a password in order to read data out of flash memory. For more information regarding secure products, please contact Macronix sales.

Security Features available in Macronix Products

Macronix memory products offer wide selection of security features to satisfy security needs of system designers. An overview of security features in Macronix products is summarized in *"Table 2. Security Features in 3V Macronix Memory"*. Secure product datasheets are available only after registration at Macronix. For detailed information, please check product datasheets or contact Macronix sales.

Table 2. Security Features in 3V Macronix Memory

Feature	Serial NOR		Parallel NOR		NAND		
	standard	**secure**	standard	**secure**	standard	standard	**secure**
	MX25Lxxx35/06	MX25Lxxx55	MX29GL	MX29GA	MX30LFxG08AA	MX30LFxG28AB	MX30LFxG28SB
OTP Area	✓	✓	✓	✓		✓	✓
SW Block Protection	✓	✓	✓	✓			
HW Block Protection (WP#)	✓	✓	✓	✓	✓	✓	✓
Advanced Block Protection	✓ Note 1	✓ Note 1	✓	✓			
Permanent Block Lock		✓		✓			✓
Read Protection		✓					
Secure BGA		✓		✓			✓

Note 1: Only for high density -128Mb/256Mb/512Mb/1Gb - 'F' revision products

Standard SW and HW Block Protection Modes

A Software Block Protection Mode (SPM) feature enables block-locking protection usually available in NOR Flash that is used to inhibit Write and Erase operations.

Using SPM, a group of flash memory blocks can be Write protected by setting specific Block Protect (BP) non-volatile flash register bits (*"Table 3. SW and HW Block Protection Modes"*, *"Table 4. Status Register and Block Protection Bits (BP) in Serial NOR"* and *"Table 5. SW Protection in MX25L6406E Serial NOR"*).

A Hardware Block Protection mode (HPM) is usually available through the use of the Write Protect (WP#) pin. When WP# is held low, the selected group of blocks will be protected and Write/Erase commands will not be accepted. In order to enable the HPM function, it is necessary to set the SRWD bit in the Status Register as described in *"Table 3. SW and HW Block Protection Modes"*.

After the programming task is done in the factory environment, the memory component might be mounted with the WP# tied to GND. As a result, no software can change the memory content anymore unless the WP# pin is de-soldered. In the MX29GL page-mode parallel NOR family the WP# pin usually can protect either the first or the last block of the memory depending on the part number. Please check the datasheet of interest for detailed information.

Table 3. SW and HW Block Protection Modes

Mode	Status register condition	WP# and SRWD bit status	Memory
Software protection mode (SPM)	Status register can be written in (WEL bit is set to "1") and the SRWD, BP3-BP0 bits can be changed	WP#=1 and SRWD bit=0, or WP#=0 and SRWD bit=0, or WP#=1 and SRWD=1	The protected area cannot be program or erase.
Hardware protection mode (HPM)	The SRWD, BP3-BP0 of status register bits cannot be changed	WP#=0, SRWD bit=1	The protected area cannot be program or erase.

Table 4. Status Register and Block Protection Bits (BP) in Serial NOR

bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
SRWD (status register write protect)	0	BP3 (level of protected block)	BP2 (level of protected block)	BP1 (level of protected block)	BP0 (level of protected block)	WEL (write enable latch)	WIP (write in progress bit)
1=status register write disable	0	Refer to *"Table 5. SW Protection in MX25L6406E Serial NOR"*				1=write enable 0=not write enable	1=write operation 0=not in write operation
Non-volatile bit	0	Non-volatile bit	Non-volatile bit	Non-volatile bit	Non-volatile bit	volatile bit	volatile bit

Table 5. SW Protection in MX25L6406E Serial NOR

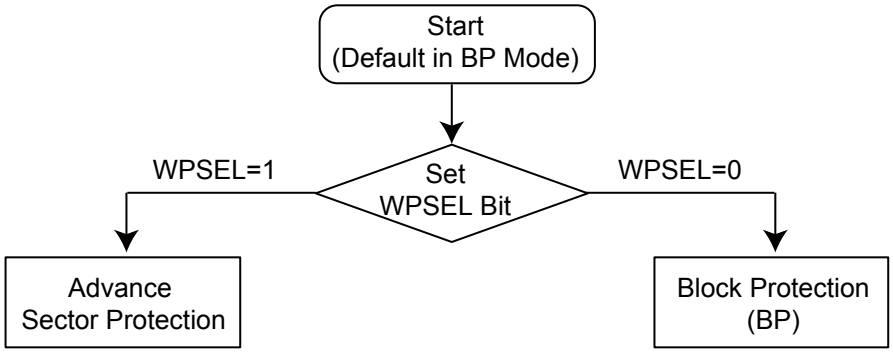
Status bit				Protect Level
BP3	BP2	BP1	BP0	**64Mb**
0	0	0	0	0 (none)
0	0	0	1	1 (2block, block 126th-127th)
0	0	1	0	2 (4blocks, block 124th-127th)
0	0	1	1	3 (8blocks, block 120th-127th)
0	1	0	0	4 (16blocks, block 112th-127th)
0	1	0	1	5 (32blocks, block 96th-127th)
0	1	1	0	6 (64blocks, block 64th-127th)
0	1	1	1	7 (128blocks, all)
1	0	0	0	8 (128blocks, all)
1	0	0	1	9 (64blocks, 0th-63th)
1	0	1	0	10 (96blocks, block 0th-95th)
1	0	1	1	11 (112blocks, block 0th-111th)
1	1	0	0	12 (120blocks, block 0th-119th)
1	1	0	1	13 (124blocks, block 0th-123th)
1	1	1	0	14 (126blocks, block 0th-125th)
1	1	1	1	15 (128blocks, all)

Advanced Block Protection Mode

Advanced Write protection mechanisms are available in Macronix high-density serial NOR flash such as MX25L12835F, MX25L25635F, MX25L51235F and the page-mode parallel NOR Flash GL Family. The Advanced protection scheme implementation is slightly different among the different product lines. The following description is given as an example and it refers to the high-density serial NOR MX25L family.

The Advanced write protection schemes can be selected by writing a One-Time programmable bit (WPSEL) in the Security Register as shown in *"Figure 3. Advanced Block Protection Mode Selection in MX25L_35F High-Density Serial NOR"*.

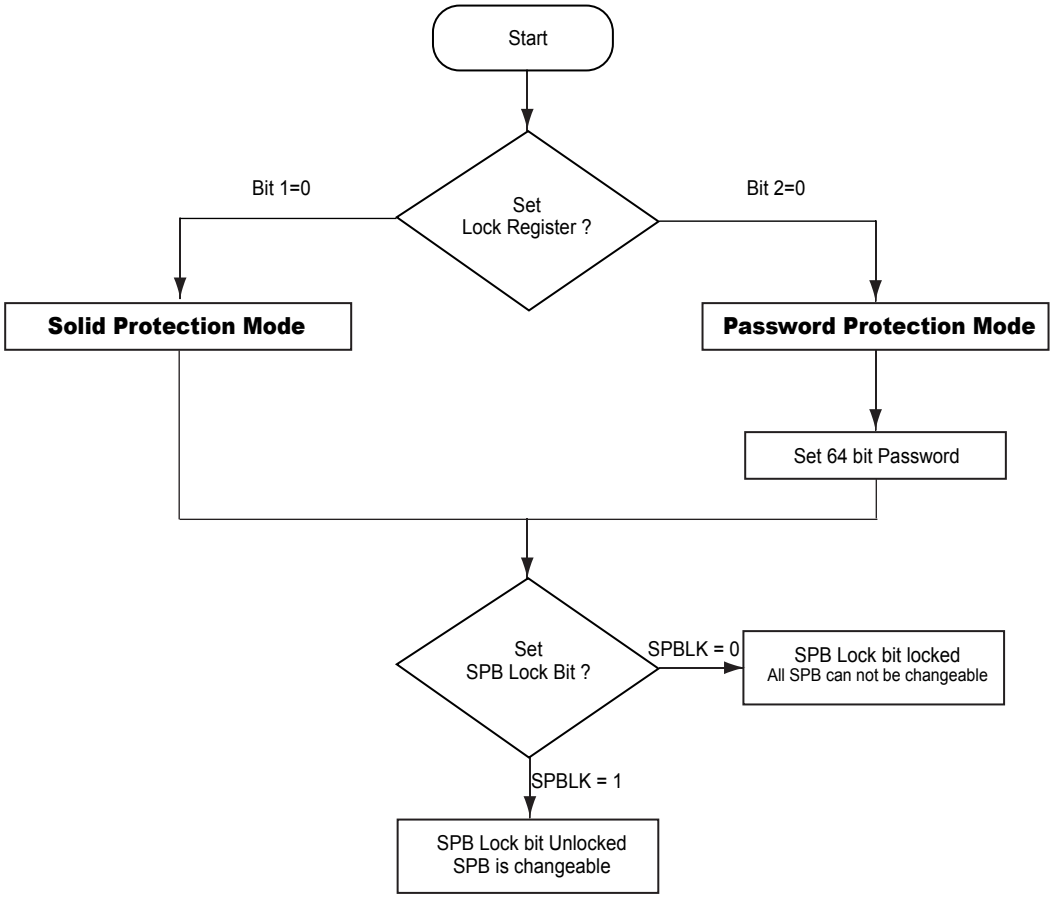
Figure 3. Advanced Block Protection Mode Selection in MX25L_35F High-Density Serial NOR



Within Advanced Sector Protection, Solid Block Protection (SBP) bits allows us to define the protection status of each block/sector by setting an associated non-volatile bit as shown in *"Figure 4. Advanced protection scheme in MX25Lxxx35F high-density serial NOR Flash"*. The power on cycle will not affect the protection status because it is stored in non-volatile elements. However, the Solid Block Protection bits (SPB) can be erased by a specific command. Dynamic Protection (DPB) volatile bits are also available and can be coupled with the SPB for flexibility. DBP volatile bits normally default to protected status after power-on and needs to be cleared by software to enable the Program or Erase commands on the block/sector.

A Password protection function is available to implement a strict lock/unlock mechanism. The Password is enabled by writing a specific OTP bit in the Lock Register as shown in *"Figure 4. Advanced protection scheme in MX25Lxxx35F high-density serial NOR Flash"*. A password chosen by the customer must be programmed inside the memory device by using a specific command. The locked sectors can be unlocked only by using the unique password defined for each memory device. Without knowing the password, intentional modification cannot take place. The password length combined with intentionally added command latency avoids the possibility of hackers trying out all the possible combinations. The Password Protected Block Locking implementation varies depending on the memory type so it is necessary to check the Macronix datasheet of interest for detailed information.

Figure 4. Advanced protection scheme in MX25Lxxx35F high-density serial NOR Flash



Once WP# = 0, all array blocks/sectors are protected regardless of the contents of SPB or DPB lock bits.

DPBs can be set or reset individually by command, or globally reset at the same time using the Gang Block Lock/ Unlock instructions. The protection is disabled if both SPB and DPB are cleared as shown in *"Table 6. Protection Scheme Block Protect Status"*.

An additional Temporary Unprotect SPB bit can be used to override all the SPBs setting by software. USPB is volatile and as such will be set to the default value after a power on-cycle. The USPB are volatile bits that allow the temporary override of the non-volatile SPB. This may be done to allow for data changes without resetting the overall configuration of the SPBs, which would require an Erase cycle and consequent reprogramming of the SPB to their original state.

Table 6. Protection Scheme Block Protect Status

Protection Status			Sector State
DPB bit	SPB bit	USPB bit	
0	0	0	Unprotect
0	0	1	Unprotect
0	1	0	Unprotect
0	1	1	Protect
1	0	0	Protect
1	0	1	Protect
1	1	0	Protect
1	1	1	Protect

In MX29GL family the advanced protection scheme is very similar to the one implemented in high-density serial NOR. One difference is that one Unprotect Solid Block Protect bit (USPB) is defined for each sector.

Advanced Write protection schemes are very effective in preventing unintentional and intentional changes to the memory content. For detailed implementation of the Advanced Protection it is necessary to check the Macronix datasheet of interest.

Permanent Block Lock

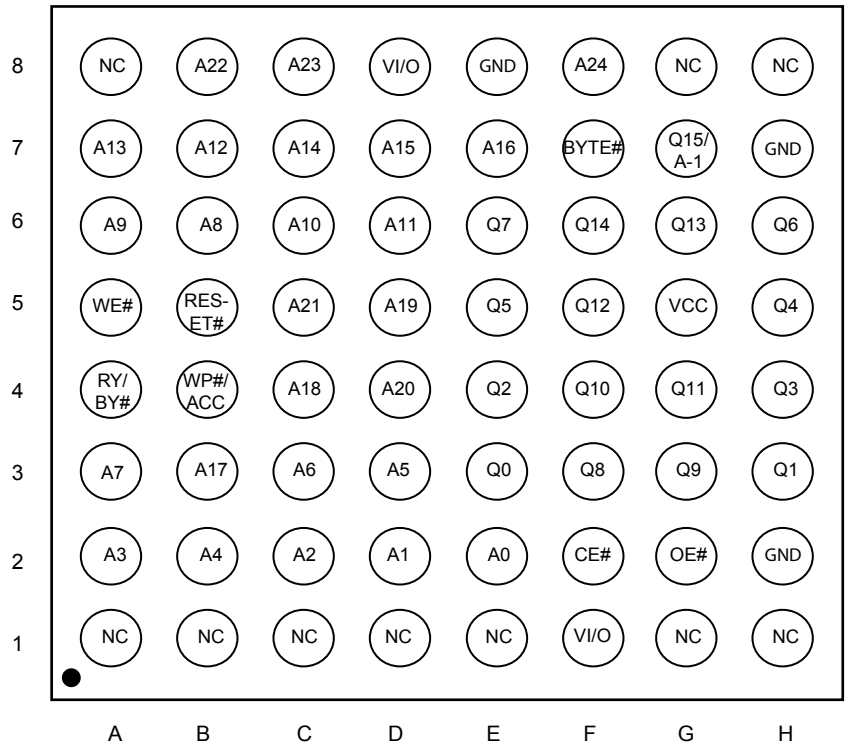
Permanent Block Lock protect is the extreme Write protection mechanism usually provided with secure products such as MX25Lxx55 serial NOR or MX29GA page-mode parallel NOR. This type of protection will allow us to overcome the weakness of the previous methods. Once a Block is permanently locked it cannot be unlocked anymore and no further changes of the locked block are possible.

The Permanent lock is available in secure serial and parallel NOR products and is also introduced on Macronix secure NAND products. For more information regarding this protection feature please contact Macronix sales.

Secure Package

Secure BGA Packages are available in Macronix secure families of NOR Flash such as MX25Lxx55 Serial NOR or MX29GA page-mode parallel NOR. The use of a BGA package - with the proper pinout which is tightly soldered onto the PCB - combined with proper PCB layout, will make it difficult for hackers to probe bus activity.

Figure 5. Secure BGA pinout example



One Time Programmable Area

A One Time Programmable (OTP) area is an extra memory space (separate from the main memory array) available in most Macronix NOR and NAND products. The OTP area can be used to store a unique ID number or other unique metadata such as a digital checksum.

Normally, serial flash are shipped from the factory with the OTP area unprogrammed (all FFh) and unlocked. Through “Special Order”, customers can request that the factory program an ESN (Electronic Serial Number) into the OTP area and then lock the OTP area so that it cannot be altered. Bit0 (Secured OTP indicator bit) of the Macronix Security Register will also be set to ‘1’ indicating that the device was factory locked. Since this bit cannot be set by the customer, cloning a factory locked device would be extremely difficult and provides a higher level of security.

The dimension of OTP area in NOR Flash varies from 512 bits to 4K bits depending on the product. *"Table 7. 4K-bit Secured OTP in MX25L12835F Serial NOR Flash"* shows the OTP area for the Macronix Serial NOR MX25L high density family. For more information regarding ESN please contact Macronix sales.

Table 7. 4K-bit Secured OTP in MX25L12835F Serial NOR Flash

Address range	Size	Standard Factory Lock	Customer Lock
xxx000~xxx00F	128-bit	ESN (electrical serial number)	Determined by customer
xxx010~xxx1FF	3968-bit	N/A	

OTP area is also offered in MX30L(U)FxG08AB Macronix NAND family and consists of 30 2KB pages.

Unique ID

The Unique ID is a unique serial number stored in each memory device. A Unique ID can be implemented by writing a serial number code into the OTP area. The customization may happen at the customer site or directly by Macronix if requested.

A Unique ID code of 32 Bytes is provided in the newest Macronix NAND products according to the ONFI command definition. The OTP operation is operated by the Set Feature/Get Feature operation to access the OTP operation mode and OTP protection mode.

Read Protection

A Read Protection mechanism is available in Serial-NOR secure products. When Read Protection is enabled, it is not possible to read data from the memory.

An unlock mechanism based on a password is necessary to unlock the memory for Read. The password will be set by the user and the password strength is such that it makes it impossible for hackers to try out all possible combinations. A power-on cycle will restore the memory status to read-protected so that in the case that the memory is desoldered from the board its content cannot be accessed. For more detailed specifications please contact Macronix sales.

Private Key Authentication

The ultimate authentication of the memory device in the system can be achieved by using a handshaking mechanism between the SoC and the memory based on secret key algorithms. Secret key based authentication / commands requires that a private / secret key be stored at the factory in both SoC and in the Memory. The Memory itself must have some cryptographic hardware in order to process the messages exchanged during the handshaking mechanism. Those Secret Key features can be used to identify the memory in the system excluding any possible counterfeit. Also, only the owner of the secret key (authorized SoC) could be enabled to send commands such as Program or Erase or Read. The secret key will be never exposed so the authentication method is extremely secure.

This type of feature is usually implemented only in special memory devices because of the cost associated with the additional hardware. Customers that may desire to implement these types of security features in their application should contact Macronix for further information.

Summary

Various aspects of System Security are discussed in this document. Security aspects deal with unintentional as well as intentional memory modification or cloning. The protection of customer IP and algorithms are also discussed. An overview of Macronix memory features that are available in order to achieve a more secure system is also given.

References

Application note	Location	Date Issued	Version
AN-0218 Serial Flash Secured OTP Area Introduction	Macronix Website	Jun. 17, 2013	0.01

Except for customized products which have been expressly identified in the applicable agreement, Macronix's products are designed, developed, and/or manufactured for ordinary business, industrial, personal, and/or household applications only, and not for use in any applications which may, directly or indirectly, cause death, personal injury, or severe property damages. In the event Macronix products are used in contradicted to their target usage above, the buyer shall take any and all actions to ensure said Macronix's product qualified for its actual use in accordance with the applicable laws and regulations; and Macronix as well as it's suppliers and/or distributors shall be released from any and all liability arisen therefrom.

For the contact and order information, please visit Macronix's Web site at: http://www.macronix.com