

Numonyx NOR flash memory securities

Numonyx® Krypto® security technologies and other security features provide protection for the system and for intellectual property



SECURITY WITH FLASH MEMORY

Numonyx flash memory offers various security methods to protect intellectual property (IP) and data.

Manufacturers around the world must protect their intellectual property (IP) in everything from consumer electronics to wired and wireless communications equipment. Protecting systems from unintentional overwrites, malicious attacks, and cloning is essential, yet it costs manufacturers and service providers millions of dollars each year.

Numonyx delivers cost-effective solutions to this growing challenge. Our expansive portfolio of security solutions enables system manufacturers to protect data from accidental or intentional corruption, as well as unauthorized IP copying or cloning. Hardware, software and combination solutions deliver the flexibility designers need to protect data or IP stored in flash, software and firmware.

Hardware protection

Hardware protection of flash requires a certain voltage to be applied to a pin on a device. This voltage will not allow modification of a block of the device, or the entire device itself.

Hardware write protection

V_{pp} or VPEN are used for complete hardware protection against program or erase on the entire array. When a valid voltage is present on V_{pp} or VPEN, the blocks in the main array can be modified. By grounding V_{pp} or VPEN, the blocks in the main array cannot be programmed or erased. Attempts to program or erase when V_{pp} or VPEN is grounded will fail,

resulting in the setting of the appropriate status register fail bit.

Available in: All Numonyx product families.

V_{pp} /WP (Write Protect) protection

This hardware method protects the highest or lowest block(s) against program and erase operations. With $V_{pp}/WP = V_{IL}$, the highest or lowest block is protected. With $V_{pp}/WP = V_{IH}$, the memory reverts back to the previous protection status of the block. Program or erase operations can now modify the data in the block unless the block is protected using block protection.

Available in: Numonyx™ Axcell™ M29 product family and M28W.

Software protection

Software provides flexible methods for volatile and non-volatile protection.

Volatile block locking

Volatile protection allows software to protect blocks against inadvertent changes. This protection can be disabled when modifications to the array are necessary. The main memory array blocks are mapped to bits in a volatile array and each bit can be individually modified. The bits in the volatile array are called Volatile Protection Bits (VPBs). VPBs can only protect blocks that are not locked with non-volatile array bits.

The VPBs can be set or cleared as often as

Numonyx NOR flash memory security features

needed. When the parts are first shipped, or after a power-up or hardware reset, the VPBs can be at the set or cleared state, depending on the ordering option chosen.

Available in: Numonyx Axcell M29 and P30/P33 product families, M58LT, and M25 serial flash product family.

Non-volatile block locking

This protection mode is for non-volatile memory. It will remain set even after sequencing the power or hardware reset.

A Non-Volatile Protection Bit (NVPB) is assigned to each block. When a NVPB is set to '0', the associated block is protected, preventing any program or erase operations in this block. The NVPBs cannot be cleared individually; they can only be cleared all at the same time by issuing a command to clear all non-volatile protection bits. The NVPBs can be protected all at one time by setting a volatile bit, the NVPB lock bit.

Attempting to erase or program in a locked block will result in a failed operation, with the appropriate bits being set in the status register.

Available in: Numonyx Axcell M29 product family, J3 product family and M25 serial flash product family. (Note: NVPB Lock Bit is not available in J3).

Software and hardware protection

The most flexible solutions combine hardware and software security measures that will support modification security as well as intellectual property security by inhibiting reads from the flash device.

Krypto® Flex Lock

Krypto® Flex Lock allows software to control block locking or it can require hardware

interaction before locking can be changed. Any block can be locked or unlocked with no latency. Once blocks are locked, they cannot be programmed or erased; they can only be read.

KRYPTO® FLEX LOCK FEATURES	
Lock block	The blocks can be locked by software only. On power-up or reset all blocks are locked.
Unlock block	The Unlock Block command unlocks locked blocks (if block isn't locked-down) so they can be programmed or erased. Unlocked blocks return to the locked state at device reset or power-down.
Locked-down blocks	<p>Locked-down blocks are protected from program and erase operations like locked blocks, but software commands alone cannot change their protection state. This feature requires the use of the WP# pin.</p> <p>WP# = VIL The lock-down command locks the block and prevents a block from being unlocked.</p> <p>WP# = VIH This overrides lock-down so that commands can change the lock state.</p> <p>The lock-down state is cleared only when the device is reset or powered-down.</p>

Table 1. Krypto® Flex Lock features

Available in: Numonyx Axcell P30/P33 product family, M28W and the Numonyx NOR for wireless W, L and M product families.

OTP space

System-level security schemes can be implemented using the OTP (One-Time Programming) space. This is a special space whose bits can only be programmed from a '1' to a '0'. OTP bits cannot be erased from '0' back to '1'. This feature makes the OTP space particularly useful for implementing system security schemes and for permanently storing data or system parameters. The bits of the OTP space are divided into two segments. One of the segments is programmed at the factory with a unique unchangeable number. The other segment is left blank for customer designers to program as desired. Once the customer segment is programmed, it can be locked to prevent reprogramming. This lock cannot be reversed.

Available in: Numonyx Axcell M29 and P30/P33 product families, M28W, M58LT, M25PX serial flash and the Numonyx NOR for wireless M product family.

System protection registers/space

This feature is available in several implementations:

The **M29W** and **M29EW** have an extended memory block. The extended block is either 64 or 128 words. It is used as a security block to provide an ID number or to store additional information.

The **J3**, **M29EW** and **M29** have an OTP Register which is a 128-bit register divided into two 64-bit segments. The first 64-bit segment is a factory-programmed segment, which contains a unique number. The second 64-bit segment is user-programmable.

M28W has an OTP register which is 128-bit user programmable and 64-bit factory programmable segment, which contains a unique number.

Numonyx NOR flash memory security features

The **P30/P33, M, L** and **58LT** implementation has seventeen 128-bit individually lockable Protection Registers that can increase system security or prevent device substitution by containing values that match the flash component to the system’s CPU or ASIC.

The first 128-bit Protection Register is comprised of two 64-bit (8-word) segments. The lower 64-bit segment is pre-programmed at the Numonyx factory with a unique 64-bit number. The other 64-bit segment is blank, as are the other sixteen 128-bit protection registers. Users can program these registers as needed. Once programmed, each customer segment can be further locked to prevent further modification.

Available in: Numonyx Axcell M29 and P30/33 product families, J3, M58LT, M28W, and Numonyx NOR for wireless L and M product families.

OTP

The OTP (One-Time Programming) feature allows designers to permanently lock blocks of a flash device so they can no longer be erased or written. This feature is widely used to protect initialization or boot code in a system so that it cannot be corrupted.

Device OTP is typically implemented by having OTP bits in a device mapped to each individual block. When a bit is programmed to a ‘0’ its associated block is permanently locked. Numonyx™ Krypto® Password Access technology adds password authentication to this feature, which helps deter OTP bits from being inadvertently set.

Available in: Numonyx Axcell M29 and P30/P33 product families, the J3 product family and M58LT.

Password protect

In this protection mode, the user can protect the entire array or select blocks in the main array from inadvertent program and erase operations. This protection mode requires a 64-bit password to be entered and the device non-volatile protection lock bit (NVPB) to be set to ‘0’. The NVPB lock bit is set at ‘0’ after power-up and reset to maintain the device in password protection mode. Successful execution of the password unlock command by entering the correct password clears the NVPB lock bit, allowing for block NVPBs to be modified.

If the password provided is not correct, the NVPB Lock bit remains locked and the state of the NVPBs cannot be modified.

Available in: Numonyx Axcell M29 family of products.

Non-volatile protection bit lock bit (global freeze bit)

The non-volatile protection bit lock bit (NVPB lock bit) is used for password protect. It is a global volatile bit for all blocks. When set (programmed to ‘0’), it prevents changing the state of the NVPBs. When cleared (programmed to ‘1’), the NVPBs can be set and reset using the NVPB program command and clear all NVPBs command, respectively.

There is only one NVPB lock bit per device. It can only be cleared by a power cycle or a reset. No software sequence unlocks this bit unless in the password protect mode.

Available in: Numonyx Axcell M29 family of products.

Krypto® Password Access

Password access will protect intellectual property stored in the main-array memory blocks by preventing reads or modification until a valid 64-bit password is entered.

KRYPTO® PASSWORD ACCESS PROTECTION MODES
Read access protect
Prevents data or code from being read from a block in the flash memory array prior to the proper password being entered.
Modify access protect
Prevents a block from being programmed or erased in the flash memory array prior to the proper password being entered.
Permanent modify protect
Prevents a block from being programmed or erased in the flash memory even if a proper password has been entered.

Table 2. Krypto® Password Access protection modes

Available in: Numonyx Axcell M29EW and P30/P33 product families, and the J3 product family.

Krypto® Encrypted Access

Krypto® Encrypted Access allows the protection of intellectual property from inadvertent or malicious modifications and the ability to read code/data. It is available in addition to other security features on certain products. This security feature uses both hardware and software to protect blocks. It can be used to prevent malicious code modifications, to hide sensitive data or to limit access to certain blocks.

/ **Modify protection** - Protects individual blocks or groups of blocks from program and erase operations. The content to be protected is configured through non-volatile modify protection bits (NVMP bits) assigned to each block/group of blocks.

/ **Read protection** - Protects individual blocks or groups of blocks from read operations. The content to be protected is configured through non-volatile read protection bits (NVRP bits) assigned to each block/group of blocks.

The devices support specific encryption algorithms. (See Table 3)

Available in: M28W family of products.

Summary

Numonyx delivers a flexible set of security features that create cost-effective alternatives to protect data and IP stored in flash, software or firmware.

KRYPTO® ENCRYPTED ACCESS PROTECTION MODES
Default mode
Blocks can be added and removed from the set of modify protected blocks. New blocks can only be added to the set of read protected blocks.
Password protection mode
A password is required before modifying the set of blocks selected to be protected from program/erase and read operations.
OTP mode
New blocks can be added to the set of blocks selected to be protected from program and erase but no block can be removed.
Freeze mode
The set of blocks selected to be protected from program/erase and read operations is frozen.
Memory authentication
This mechanism prevents on-board flash substitution.

Table 3. Krypto® encrypted access protection modes

Learn more

For additional information about Numonyx Krypto Security Technologies and other security features, please contact your Numonyx sales representative, or visit us online at numonyx.com.