A MICRON
TECHNICAL
MARKETING
BRIEF

NAND Security Solutions for Set-Top Boxes

Overview

Set-top boxes (STBs) are an integral component of today's home entertainment and information delivery systems.

A typical STB architecture, as illustrated in the diagram below, includes an A/V decoder (processor) that decodes the encrypted digital signals and converts them to audio and video signals. As demand for premium, 4K UHD content, uninterrupted video-on-demand, and multiple screens grows, STBs are becoming increasingly processor- and memory-intensive.

For multi-service operators (MSOs), unauthorized viewing of content and tampering with STB software are the main concerns. Consequently, STB security is a top priority for them.

MSOs require STBs to be certified with conditional access system (CAS) to protect the content they broadcast. The CAS works by authenticating the communication link between the STB and the MSO network. The authentication process involves complex handshaking mechanisms and specialized codes that are stored on a highly secure nonvolatile flash memory inside the STB instead of the smart cards used in earlier versions of the CAS. Any attempt to clone the memory or bypass the authentication process will render the STB useless, providing further incentive to keep the codes safe.

MSOs also want to prevent hacking of the STB software, which can cause the device function in ways other than what is intended. Therefore, protecting an STB involves preventing unauthorized access or modification of the system boot, operating system, and application software, all of which have to be stored in a secure nonvolatile flash memory. This technical marketing brief specifically addresses the security solutions for NAND flash memory used in STBs.

Nonvolatile Memory Architecture for Set-Top Boxes

Traditionally, NOR flash was the first choice nonvolatile memory used by STB manufacturers who preferred to use it for storing software because of its extensive security features. As STBs became more memory intensive, NAND flash was added to store the noncritical software and data. But a standard NAND flash device lacks the security features needed to protect an STB.

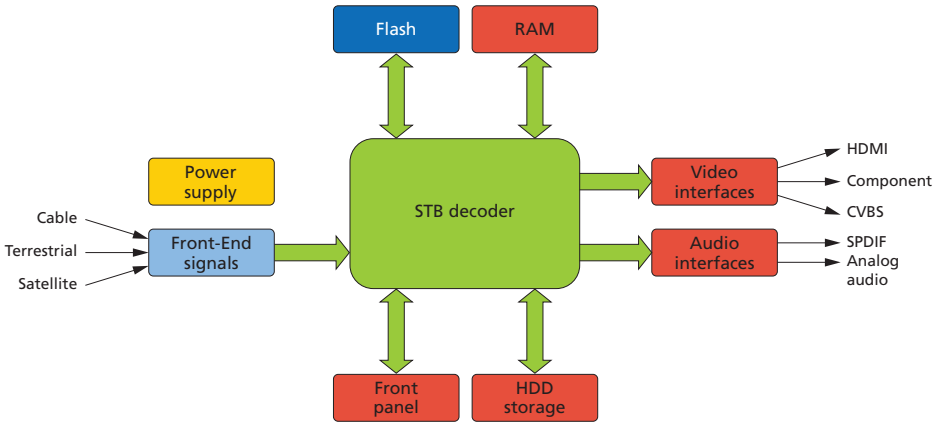

Figure 1: Typical STB Architecture

With the introduction of NAND flash devices with security, STB manufacturers can now consolidate and simplify their design by using just one NAND flash device that can store critical software such as authenticated system boot or OS, as well as noncritical software and data.

The figure below shows an optional usage of a NAND device with security in an STB and its interaction with the processor (SoC). NAND devices with security store an authenticated system code used for decrypting the content signals received by the STB. Some STB manufacturers also store additional specialized codes to make the encryption mechanism stronger. This security management system ensures that only authorized subscribers can access the licensed media content.

NAND devices with security provide the flexibility of permanently or temporarily locking groups or blocks of memory such as boot software, system libraries and the operating system. It ensures the integrity of these regions of memory by making them temporarily or permanently tamper-proof. NAND devices with security can also store a locked, unique digital signature for the STB, containing details such as the vendor ID, production data, etc. This signature helps the STB processor authenticate the nonvolatile storage and discourages memory cloning. The authentication scheme ensures the integrity of all reads from the NAND device with security. It also helps the STB processor recognize that it is communicating with the correct memory device.

Features and Advantages of NAND Devices With Security

Standard NAND devices provide only a write protect pin, whereas NAND devices with security offer a host of additional software and hardware security features which prevent unauthorized or inadvertent programming and erasing of the flash memory. Features include:

- **Write Protect:** A basic, temporary security feature whereby the entire device can be locked/unlocked by toggling a hardware pin.
- **Block Lock:** As the scope and size of STB software increases, areas of the software such as boot, operating system, MSO applications and non-critical data need different access levels. Block lock is a temporary security feature that works in conjunction with the LOCK hardware pin, offering the flexibility of locking certain groups of memory blocks. If the LOCK pin is high on startup, the entire flash array is locked and the

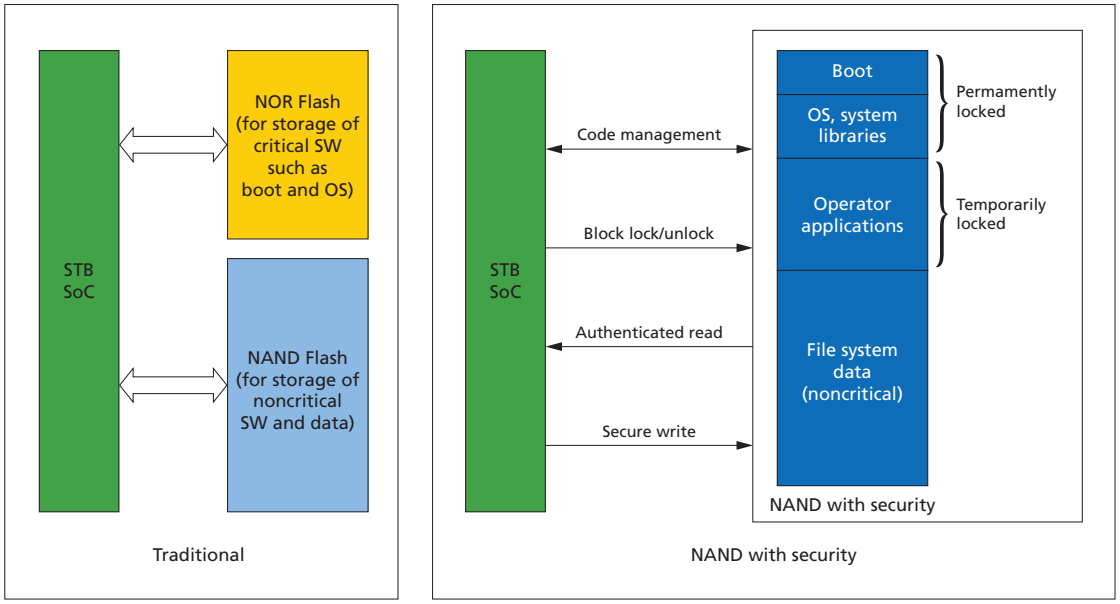

Figure 2: Comparison of NAND With Security and Traditional STB Nonvolatile Memory Architecture

UNLOCK command should be used to unlock the memory blocks that don't need protection against PROGRAM and ERASE operations. To reverse the unlocking of these blocks, the LOCK command can be issued, which will lock all the blocks on the device.

- **Lock Tight:** A software command that prevents locked blocks from being unlocked and also prevents unlocked blocks from being locked. When this command is issued, the standard lock and unlock commands are disabled. This feature prevents inadvertent program or erase operations of the flash. The LOCK TIGHT command can be activated only if the write protect and the lock pins are both set high.
- **Permanent Block Lock:** A software-enabled feature that protects certain blocks of memory permanently. It is ideal for stable and critical code such as boot, operating system, and system libraries. Permanent block lock ensures that these regions of memory can't be modified once the STB manufacturer locks the data.

FEATURE	HARDWARE-ENABLED	SOFTWARE-ENABLED
Write Protect	✓	–
Block Lock	✓	✓
Lock Tight	–	✓
Permanent Block Lock	–	✓

Table 1: Features of NAND Devices With Security

Standard NAND flash typically offers block 0 as valid upon shipment, while NAND devices with security offer blocks 0–7 as valid to provide enough capacity for customer to store copies of their critical code in case any block turns bad during the life of the NAND flash. Hence, it serves as a reliable method for booting the device while also simplifying the design of the software by reducing the need for complex error management. Using a NAND device with security in a ball grid array (BGA) package further enhances security by making it harder to probe signals at the memory pins.

Multi-Service Media Gateways

An emerging trend in the media and telecommunications industry is the multi-service media gateway, which combines the functionality of a modem, a router and a gateway for the Internet of Things (IoT) into one device. Consequently, future home entertainment and information delivery systems could consist of just this gateway and a compact IP-STB. As more systems such as home lighting, thermostats, access control, etc., get connected to the Internet via the media gateway.

The Need for On-Die ECC and Micron's SLC NAND With Security

ECC complexity increases due to lithography changes. Host has to support appropriate ECC depending on technology. Frequent technology migrations pose significant changes to host as it has to keep up with new ECC requirements. Micron offers SLC NAND with ECC built-in, removing the ECC burden on the host side. Internal ECC is enabled with ONFI SET feature or by factory trim. Our latest SLC NAND offering comes with the security features discussed in this document, making them an ideal solution for secure applications.

SLC NAND With Security:
- » High performance
- » Parallel and SPI interface
- » 1.8V and 3.3V support
- » Wide temperature offerings
- » Security features
- » Drop-in compatibility
- » Ease of use
- » Low-/mid-density offerings

Conclusion

NAND devices with security provide a simple, comprehensive and secure memory solution for set-top boxes and are equipped to handle the security needs of media gateways in the future.