Securing Digital Content with Embedded Non-Volatile Keys

Joel Rosenberg, Sr. Marketing Director
Virage Logic Corporation
Joel.Rosenberg@Viragelogic.com
(510) 360-8096

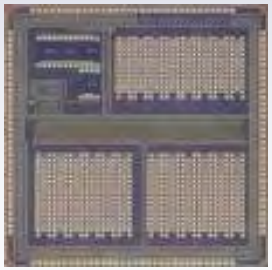
Market Trends
Digital Content

- The creation and distribution of digital content such as music and video is growing rapidly
  - Internet Protocol TV (IPTV) for services such as video on demand
  - Digital content is key to applications such as DVD players, set-top boxes, HDTV and all-in-one handheld devices
- Consumers are seeking flexibility in where and how they play this content

Addressing Security Challenges

- The greatest challenge for digital content producers is protecting their revenue streams against piracy
- A system is only as secure as the secrecy of the encryption key
  - Software systems are not secure and eventually are hacked
  - To address the lack of security in SW, encryption keys are being embedded in hardware
    - Embedded in non-volatile memory (NVM) on the SoC
  - Multi-time programmability provides greater security
    - The key can be altered *before* the attacker can exploit it

Un-secure



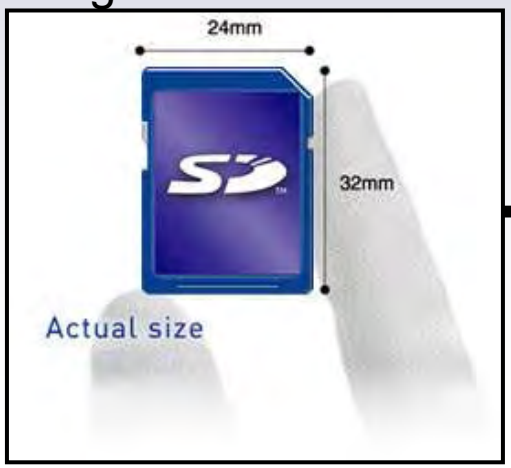
Secure

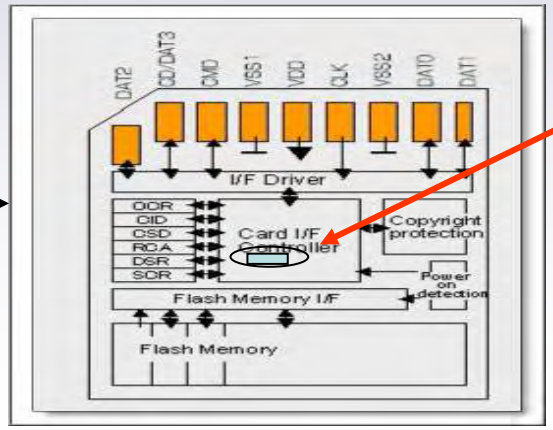
Secure Applications:
HDTV & DVD

- HDTV/DVD Chip System-on-Chip (SoC) suppliers must provide pre-keyed chips for HDCP, AACS
  - SoC supplier can securely provide
    - Embedded encryption keys (e.g. KeyInject™)
    - Secure cryptographic cores
  - SoC supplier can sell "pre-keyed" devices at a premium
    - Ability to modify embedded key in-system adds value
- Embedded NVM enables rapid time to production & modifications for SoC supplier
  - Automatic Security Development Environment for HDTV/Device
  - Enables Pre-keying

Secure Application:
Secure Flash Memory Cards

- Mobile phones, laptop computers, and video players all utilize secure Flash memory cards to allow portable usage of digital content
- Flash Controller Chip can store the following in embedded NVM
  - Encryption keys
  - An integrity checksum to prevent re-flashing of the content
    - This integrity checksum can be updated each time the content changes

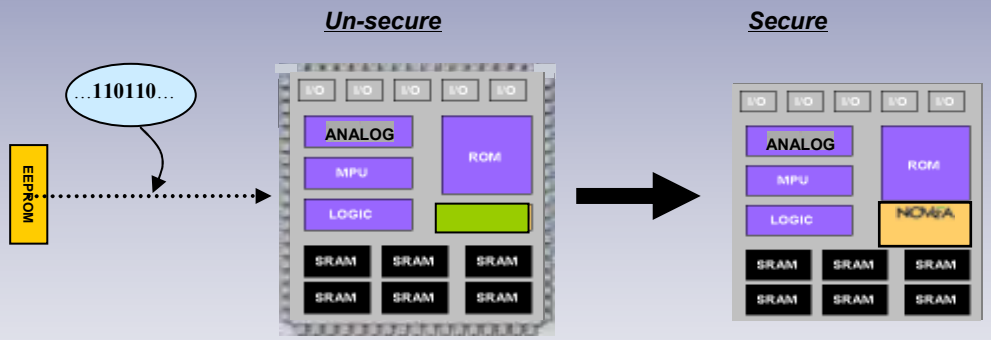




Secure NVM

Security Is in the Key

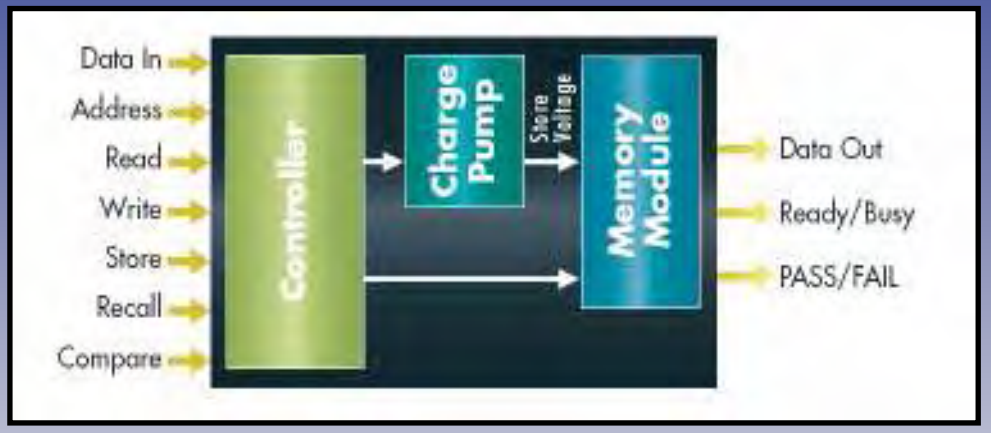
- Kerckhoffs' principle of cryptography
  - "The enemy knows the system"
  - "Only secrecy of the key provides security"



- Easier to protect the key than the algorithm
  - First line of defense is an embedded key in the controller
- With a multi-time programmable solution the key can be altered *before* the attacker can exploit it

NOVeA Memory System with Compiler
Complete Embedded NVM Solution

- NOVeA Deliverables
- Memory Module (GDS)
  - SRAM & NVM Modules
  - Up to 16K bits
- Charge Pump
  - Generates regulated high voltage for STORE operation
- Controller
  - Controls the Charge Pump and Memory Module
  - Facilitates timing and functionality tests
- Completes Design Flow Integration
  - .LIB, .LEF
  - Verilog, VHDL
  - Cadence, Magma, Mentor, Synopsys, . . .



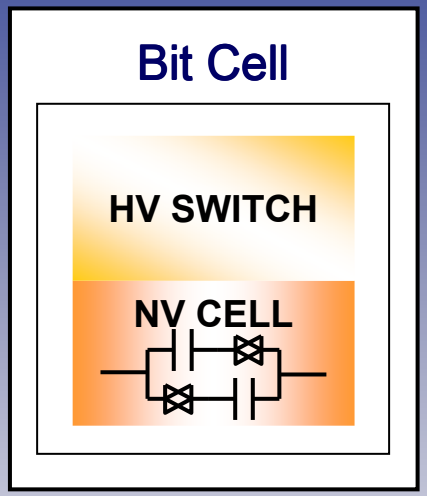
	Size Range (Total # of bits)	# of Words	# of Bits per word
Memory Module	32 – 16K	4 – 128	8 – 128

Memory Compiler

➢ ***Complete solution for embedded NOVeA design and integration***

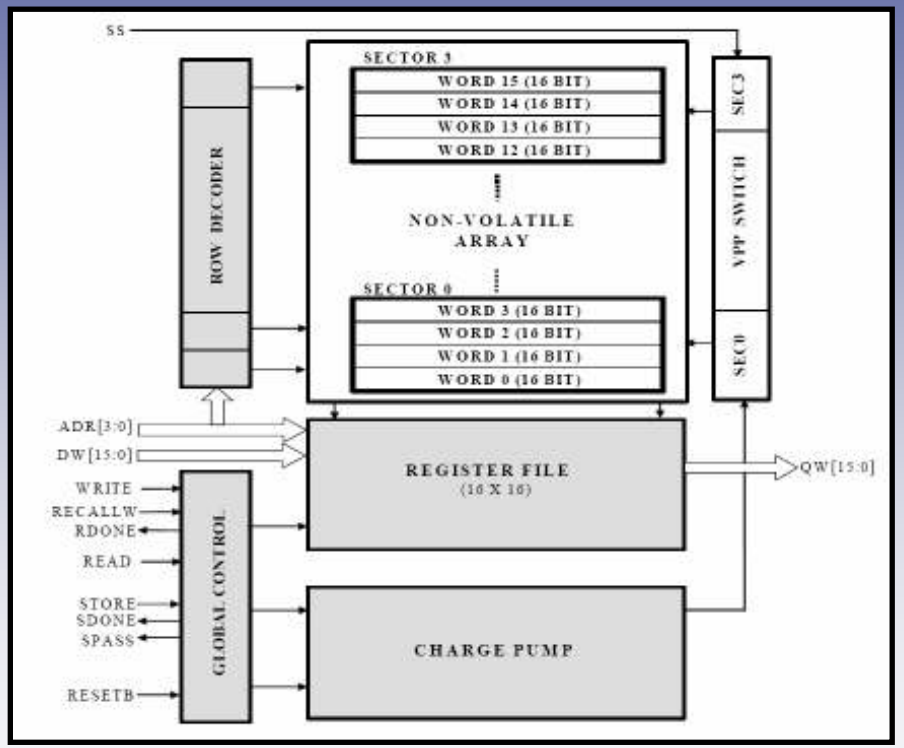
Designed for Maximum Yield & Reliability

- Each memory bit cell has its own read and write circuitry
  - Each cell is totally self-contained and isolated
  - Avoids “neighbor effects”
  - Complete immunity to “read and write disturbs”
- Dual cell approach allows differential read and with very low sense margin required
  - Reliable operation for a wide range of oxide quality
  - No process “tuning” required
- Dual cell approach also provides 100% redundancy
  - Ensures extremely high yield
- Proven successfully across multiple foundries and technology nodes – 0.18 um, 0.15 um, 0.13 um, 90nm



NOVeA Availability
7 Foundries, 8 Technology Nodes

- **CHRT 0.13 µm G/HVT**
- **IBM 0.18 µm MM (7RF)**
- **NEC 0.15 µm G**
- **Tower 0.18 µm G, MM**
- **TSMC 0.18 µm G, MM**
- **TSMC 0.13 µm G, LV-OD**
- **TSMC 90nm G, LP**
- **SMIC 0.13 µm G**
- **UMC 0.18 µm G**



Summary

Secure *Content Protection for Digital Consumer Applications*

- Advanced Access Content System (AACS) is used in content protection for HD-DVD and Blu-ray Disc
  - AACS was reportedly breached on a software DVD player by extracting the encryption keys from main memory
  - NOVeA can be used to help protect against this type of attack
- High-Bandwidth Digital Content Protection (HDCP) provides content protection over a High-Definition Multimedia Interface (HDMI) in Set-top boxes, DVD players and DTV
  - NOVeA can be used to store updated revocation list

Thank you!

Joel Rosenberg, Sr. Marketing Director
Virage Logic Corporation
Joel.Rosenberg@Viragelogic.com
(510) 360-8096