SPANSION™

Securing Flash Technology

Dr. Elena Trichina, Spansion International

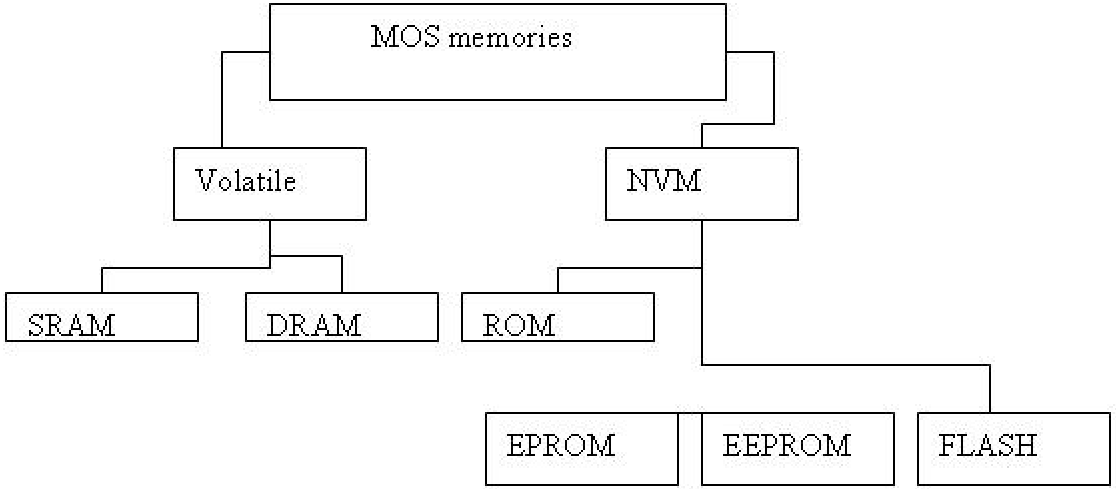
Dr. Helena Handschuh, Spansion EMEA

Memory

- All computer-based systems contain memory where information is stored while waiting to be operated on by the Central Processing Unit (CPU) of the computer
- There are two types of memory: volatile and nonvolatile
  - Operating instructions are in nonvolatile memory
  - RAM used as a read/write working storage
  - Bulk storage in cheaper serial access media (disc or tape)
- Memory may be embedded or discrete
- System design dictates actual memory needs
  - Design parameters: speed, density, cost, von-volatility, read/write, electrical parameters, power, reliability, form-factor, operating conditions, time to market …

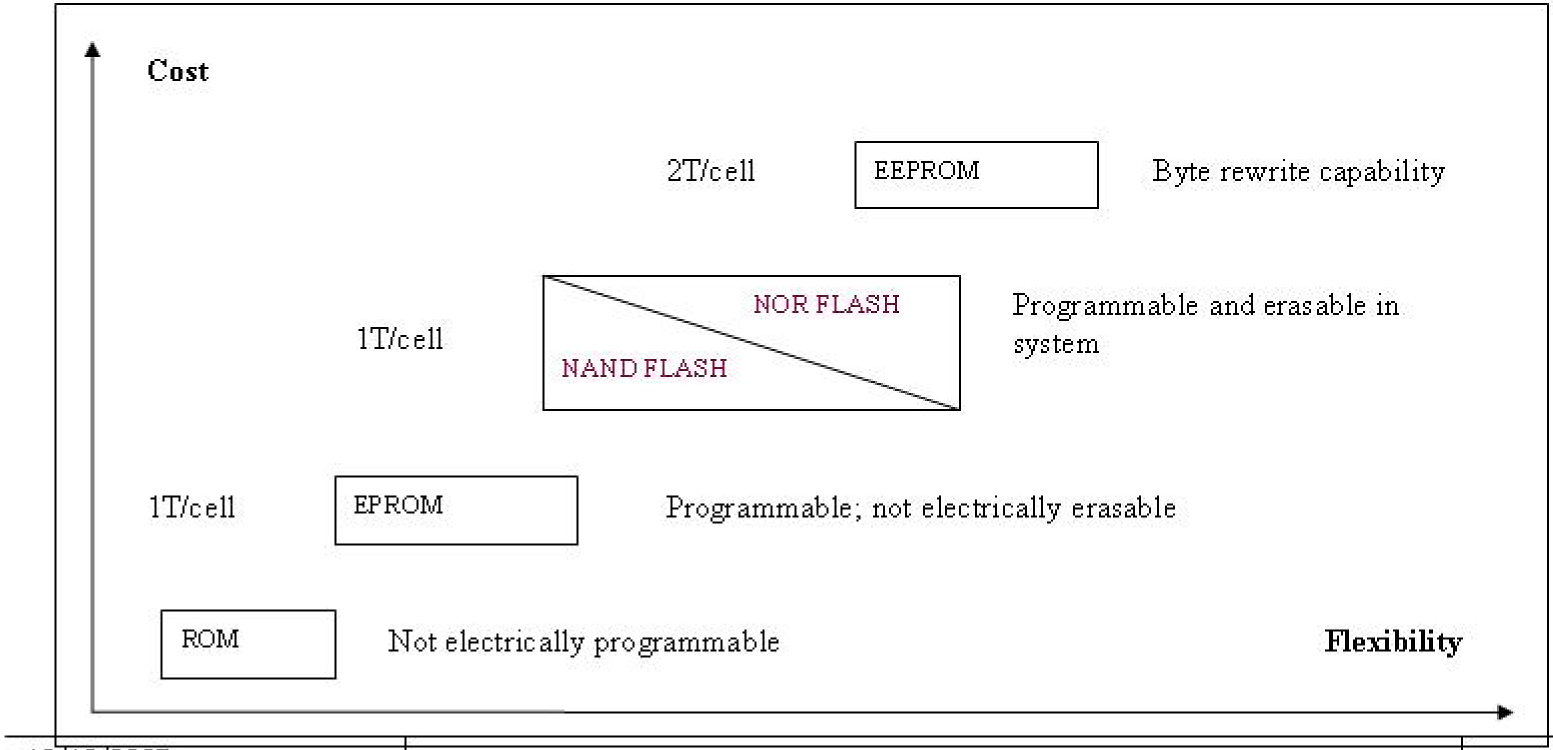
Semiconductor Memories

- Volatile memories, although very fast in writing and reading (SRAM) or very dense (DRAM), lose data content when the power supply is turned off
- Nonvolatile memories, like EPROM, EEPROM, Flash are able to balance programming and reading performances with the capability to keep the content without power supply



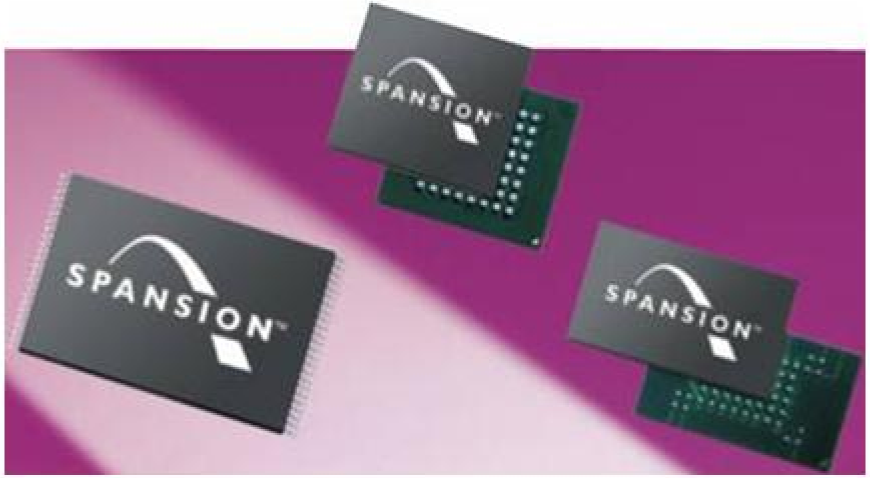
Flexibility-Cost Analysis of NVM

- Flexibility means the possibility to be programmed and erased many times on the system with minimum granularity (whole chip, page, byte, bit)
- Cost means process complexity/silicon density, or cell size



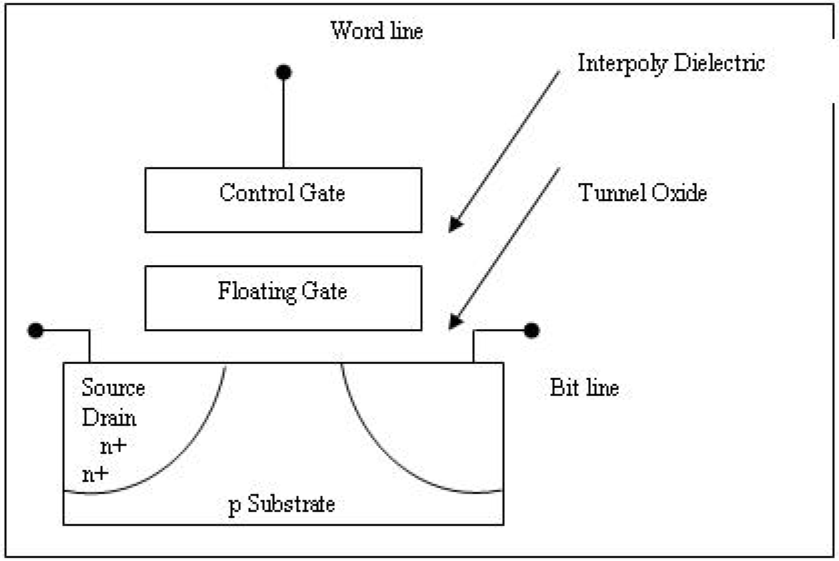
Cost
2T/cell
EEPROM
Byte rewrite capability
1T/cell
NOR FLASH
NAND FLASH
Programmable and erasable in system
1T/cell
EPROM
Programmable; not electrically erasable
ROM
Not electrically programmable
Flexibility

Flash Technology



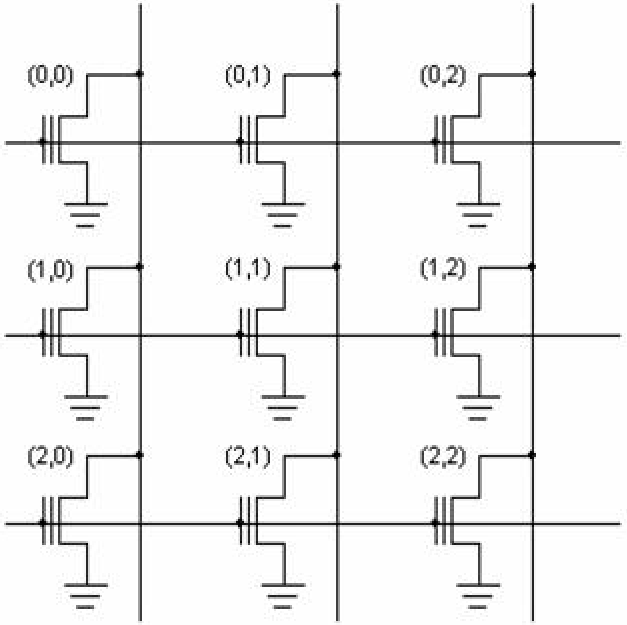
Flash Cell Basic Structure

- A flash cell is floating-gate MOS cell, i.e., a transistor with a gate completely surrounded by dielectrics (FG), and electrically governed by a capacitively coupled control gate (CG).
- Being electrically isolated, FG acts as a storing electrode for the cell: charge injected into FG is maintained there
- The gate dielectric between the transistor channel and the gate is an oxide, 8-10 nm and is called tunnel oxide
- The dielectric separating FG/CG is formed by oxide-nitride-oxide
- The floating-gate structure is common to all NVM cells based on the MOS-transistor



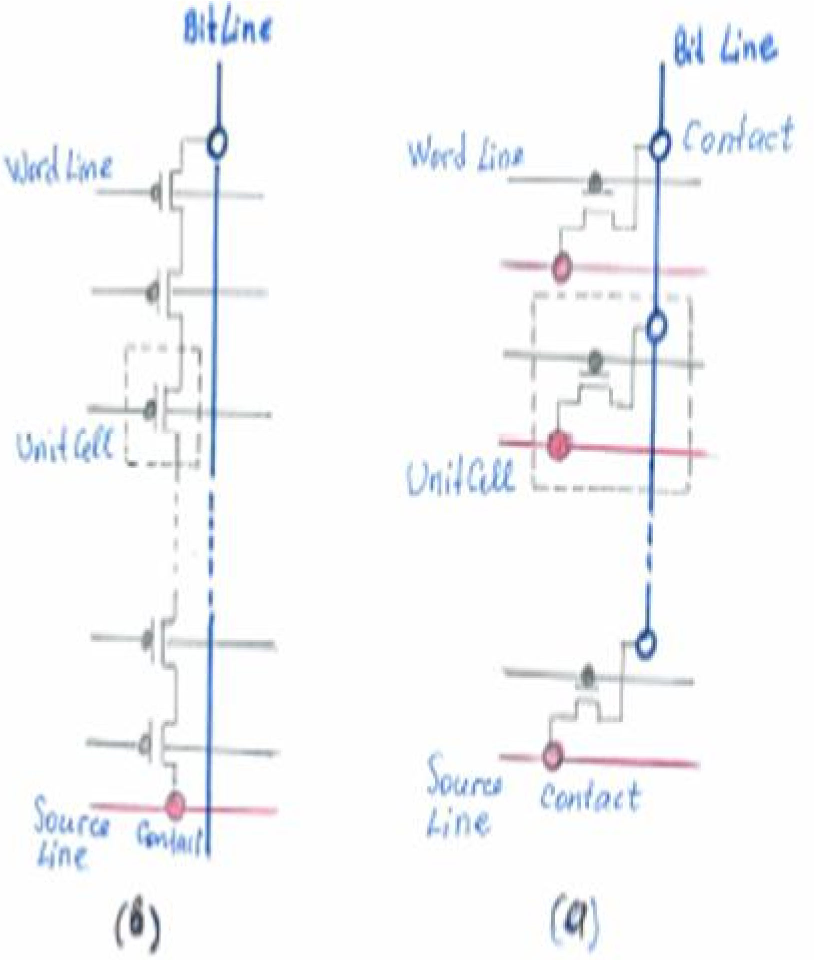
Memory Array

- To achieve a high density of the device with a relative ease of manufacturing, cells have to be arranged in structured manner, normally in an array
- Each cell can be specified by its row and column address
- The device translates the linear address presented on I/O lines into a row-column address (decoding)
- Columns of cell all share metal 1 common drain connection called a bitline (BL)
- Rows of cells share common poly-2 gate connection called a wordline (WL)
- Bitlines and wordlines allow a means for placing the appropriate voltages on each cell individually or in groups as required by the operations.



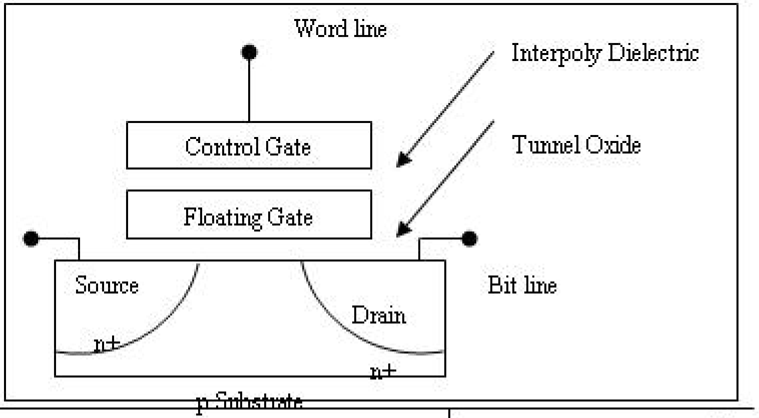
NOR and NAND

- NOR flash name is related to the way cells are arranged in an array (a), through rows and columns in a NOR-like structure: if any memory cell is turned on by the corresponding word-line, the bit-line goes low.
- NOR flash requires 1 transistor for every contact (one drain contact common for two cells); the source electrode is common for all cells
- Sacrificing random access, denser memory can be achieved by arranging 8/16/32 memory transistors in a series (b). This is typical for NAND flash organization



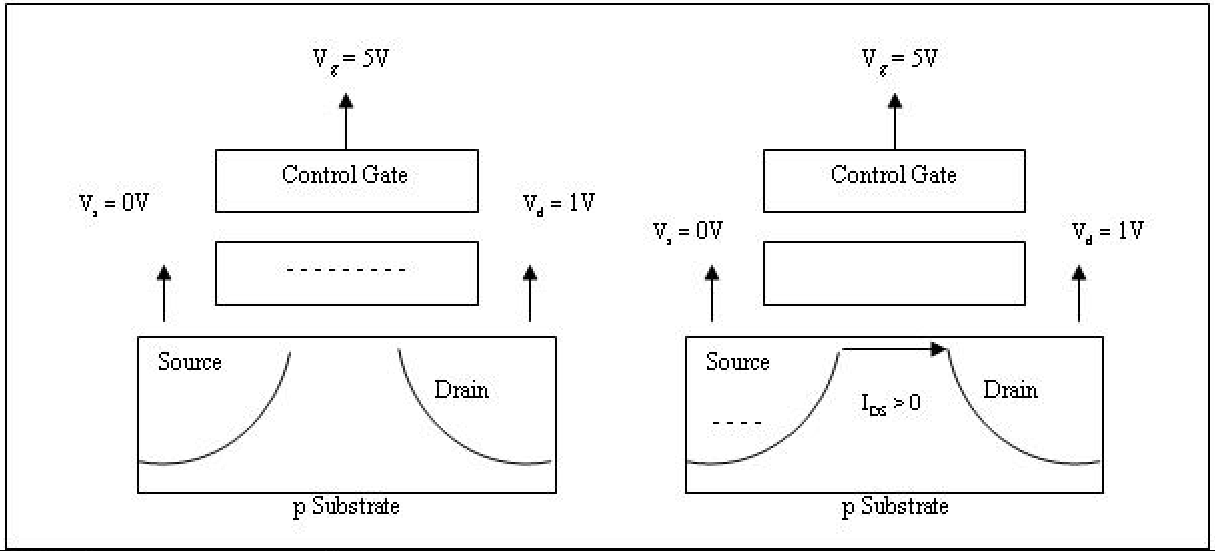
Threshold Voltage

- In a neutral state, there is no conductive path between the drain and the source.
- When a positive charge is applied to the gate and the drain, a channel begins to form between the source and the drain.
- When the CG voltage is sufficiently large the channel is formed, and electrons flow from the drain to the source, creating a current, I_{DS}.
- The voltage at which the channel forms is called a threshold voltage of a transistor, V_T



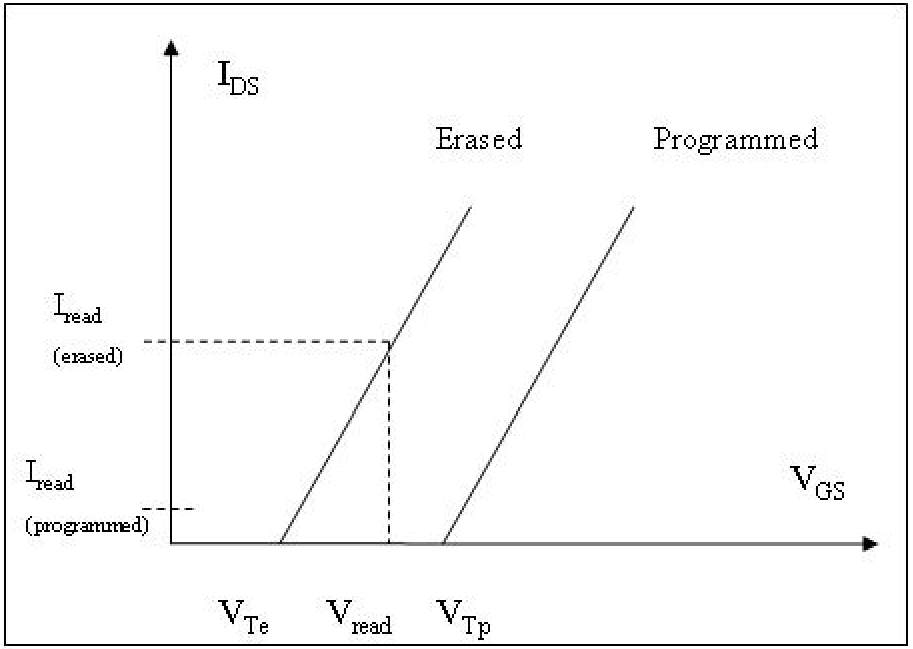
Programmed and Erased Cells: 0/1

- When a charge is stored on a FG, the threshold voltage increases; this increase is proportional to a stored charge.
- We define a logical state "1" from a microscopic point of view as no electron charges stored in the floating gate
- Vice versa, the logical state "0" is defined by electron charge stored in the floating gate



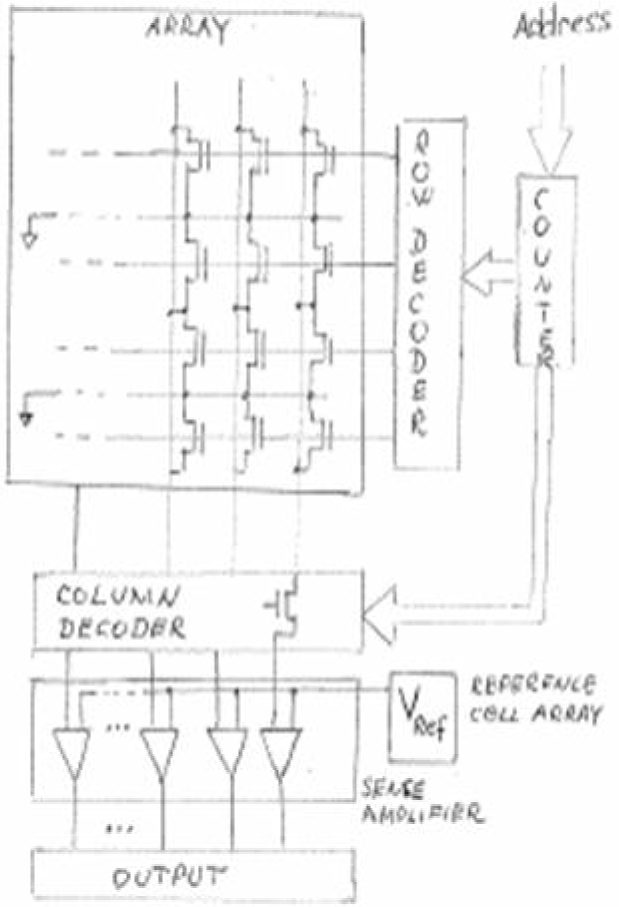
Read Operation

- The cell has basically two threshold states, a programmed state (V_{Tp}) and an erased state (V_{Te})
- The read voltage V_{read} is selected in between V_{Tp} and T_{Re}
- If current flows at V_{read}, then the cell is read as erased ("1")
- Thus the state "1" from macroscopic point of view is defined as a large (tens of microampere) reading current
- The state "0" is defined as zero current
- To read a value, we must determine the relative threshold voltage of a cell and compare it to a standard reference



Sense Amplifiers & Reference Cells

- To read the value of a cell, we must determine the relative threshold voltage of this cell and compare it with a reference
- For this, we need a means of measuring current and have reference cells for comparison
- The reference cells dictate the boundaries where the cell is considered programmed or erased by relating the measured V_T of a cell against appropriate (V_{read}, $V_{program\text{-}verify}$, V_{erase}) reference
- This process is accomplished by sense amplifiers

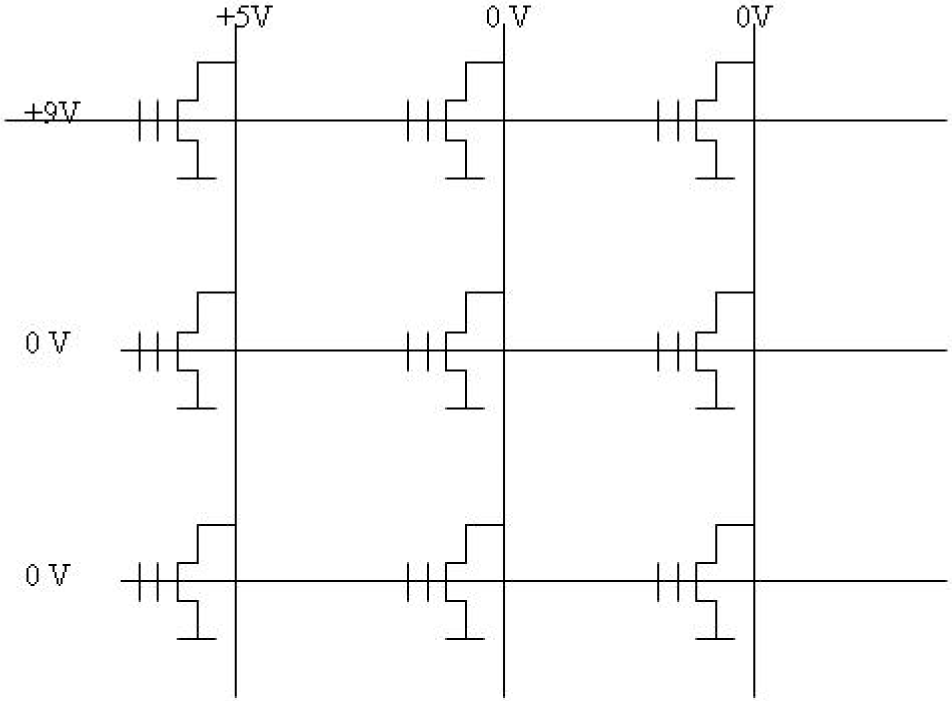


Program/Erase Operations

- How charge can be moved to and from a floating gate?
- This can be done by exploiting different physical effects:
  - The CHE mechanism, where electrons gain enough energy to pass the oxide-silicon energy barrier thanks to the electric field in the transistor channel between source and drain
  - The Fowler-Nordheim electron tunneling mechanism, i.e., a quantum-mechanical tunnel induced by an electric field. Applying a strong (8-10 MV//cm) electric field across a thin oxide, it is possible to force a large electron tunneling current
  - The photoelectric effect, where electrons gain enough energy to cross the barrier thanks to the interaction with a photon energy (which corresponds to UV radiation) larger than the barrier itself. This mechanism is the one originally used in EPROM to erase the entire device
- A common NOR flash is programmed by CHE injection at the drain side and is erased by FN tunneling through the tunnel oxide from FG to the silicon surface

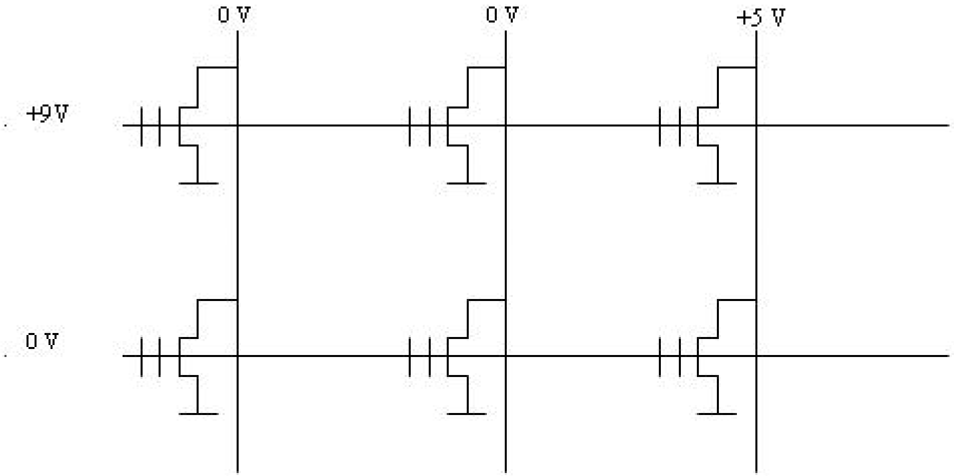
Programming in the Array (1)

- To program an individual cell, its drain connection (bitline) must be of an intermediate potential and its poly 2 gate (wordline) must be *pulsed* at a high potential
- *Programming is self-restricted in nature*



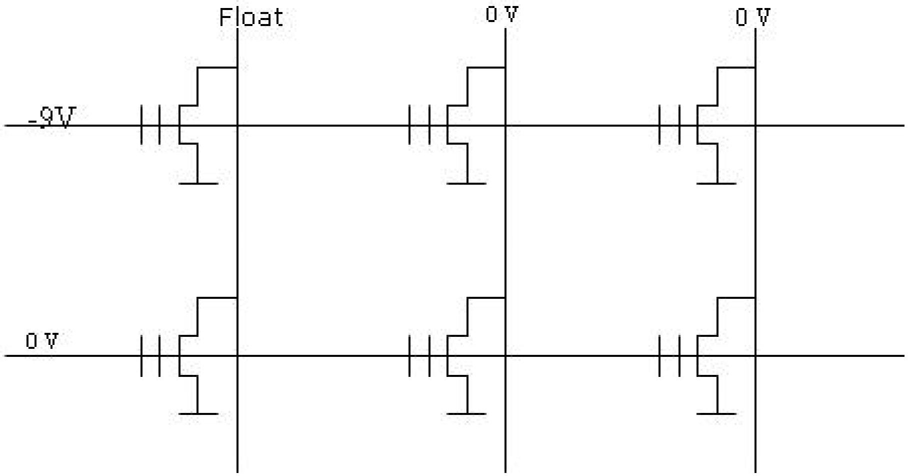
Programming in the Array (2)

- How to prevent other cells in an array from being programmed?
  - A high drain bias must be used to cause significant current flow in a channel so that electrons gain sufficient energy
  - All we have to do is to hold the drains of other cells on the wordline at ground potential so that they do not program along with the selected cell. For example, if we program cell (0,2), the bitlines of cells (0,0) and (0,1) must be held at 0V (ground)



Erasing in the Array

- In order for FN tunneling effect to perform, a high negative current must be applied to the gate, and the drain is left floating with the source tied to a positive potential through an erase load
- At this conditions, the cell X/Y will erase, but what about other cells which share the wordline?
- If they were all programmed, they also begin erase
- In non-programmed cells, hole-electron pairs also will begin to separate from FG, and the cells become ***over-erased***

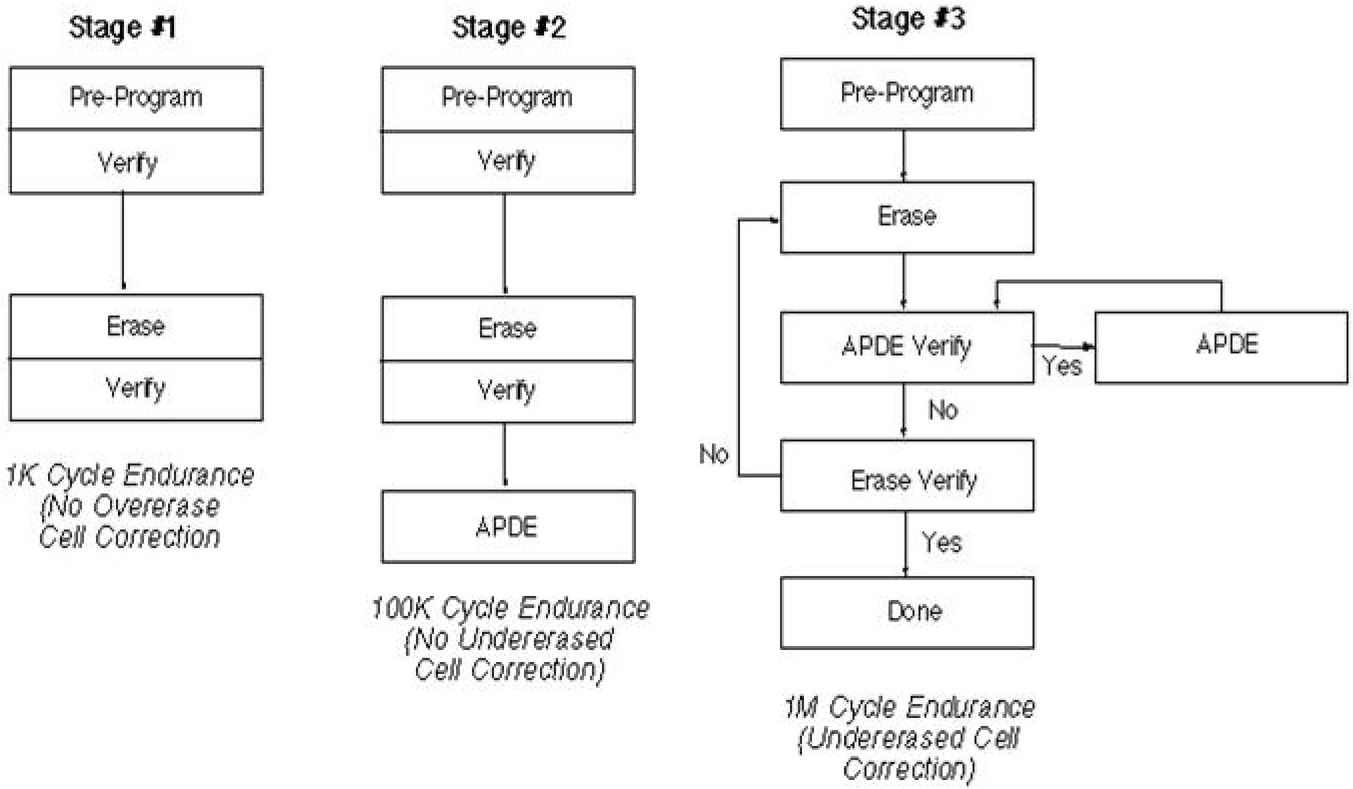


- *We can only erase cells on an entire row basis*
- *All cells in a row must be programmed before they can be erased*
- Different cells erase at different rate; APDEV read is performed on a cells after every erase pulse so that column leakage can be corrected

Erase Algorithms and Reliability

- Methods to fix over-erased (2) and under-erased (3) cells

How [redacted] Overcame Endurance Failures



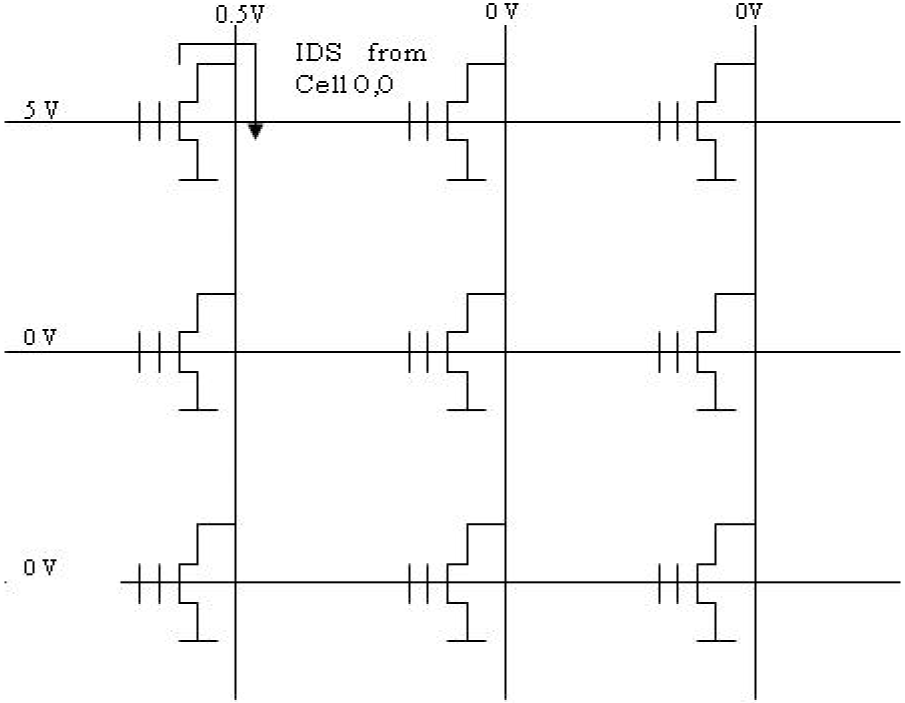
1K Cycle Endurance (No Overerase Cell Correction

100K Cycle Endurance (No Undererased Cell Correction)

1M Cycle Endurance (Undererased Cell Correction)

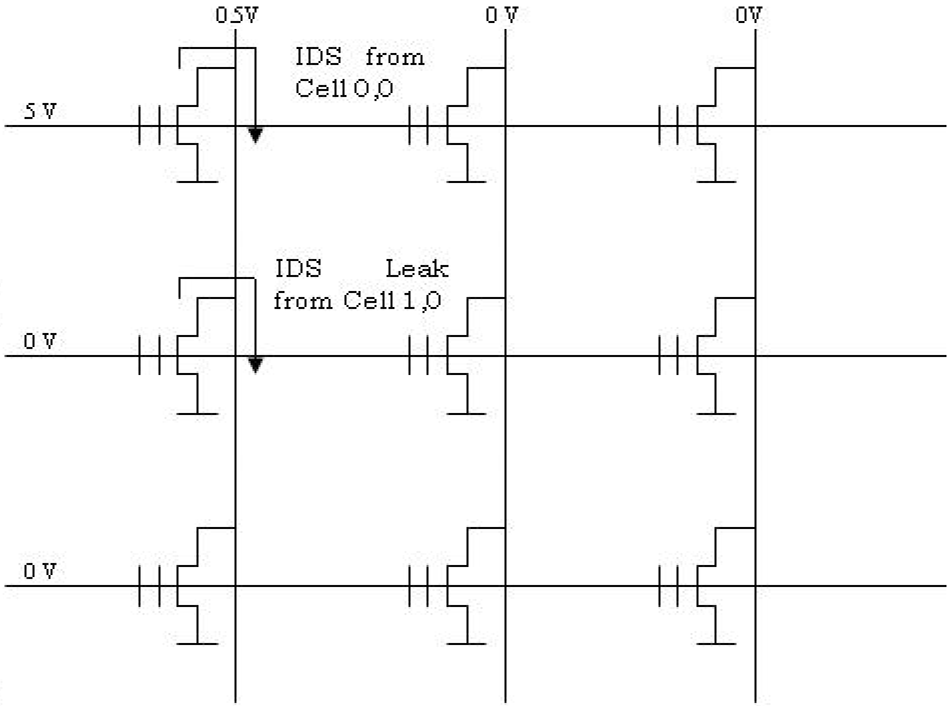
Reading the Array

- Each bitline ends up connected to a sense amplifier so that programming, erasing and reading operations can take place
- To read an individual cell, the read conditions are placed on individual bitlines and wordlines; and the current is measured and compared to read reference cell
- If the cell Row 0 Column 0 is programmed, its apparent V_T has been raised, thus it has a low I_{DS} current under normal read conditions (this I_{DS} is dictated by the PGMV reference current)



Reading: Effect of Column Leakage

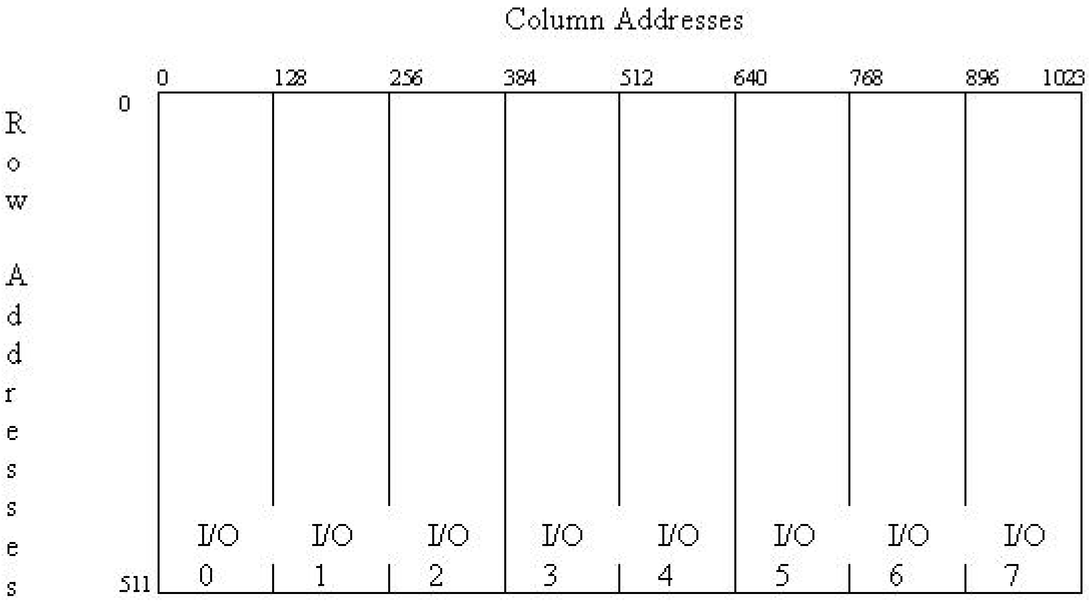
- If the cell at Row 1 Column 0 was over-erased (i.e., there is a positive charge on FG seen as a positive V_{GS} potential), a sense amplifier sees the sum of currents entering bitline from all the cells in that column.
- If this sum is larger than RDV reference, the zero will be interpreted as a false one.
- Thus it is a of a vital importance to correct any residual column leakage both during and after erase operation



Typical Array Organization: I/O

- A flash device has 8 or 16 I/O lines through which data can be programmed or read. This data is derived directly from sense amplifiers, so that bitlines carry the data to and from array
- The individual metal 1 bitlines are grouped into I/O groups; a typical number is 128 bitlines per group → 1024 bitlines/sector

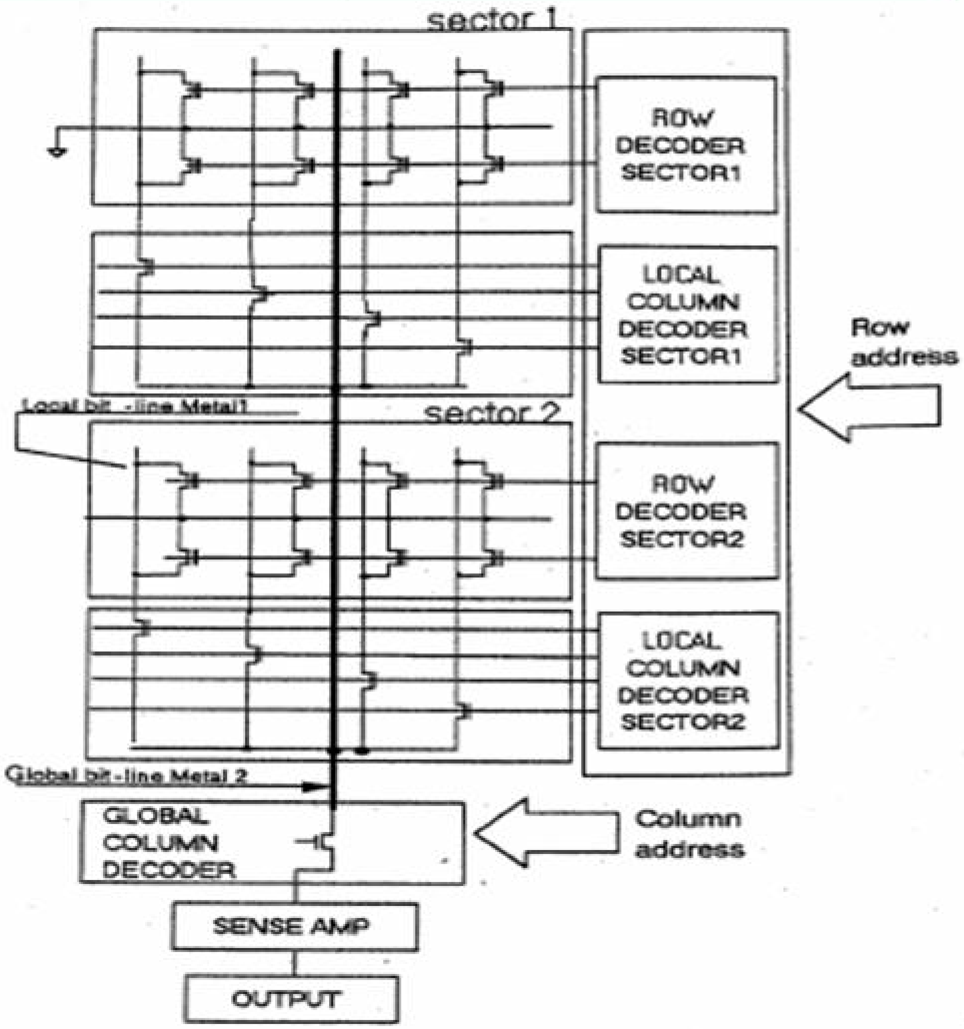
- *Translation from a linear address to X/Y address is called X/Y decoding*
- *When voltage is placed on a wordline, all cells in a row see it. If we organized an array so that all 8 data bits of an input byte lay on the same wordline, we can read them at the same time*



Sector Array Organization

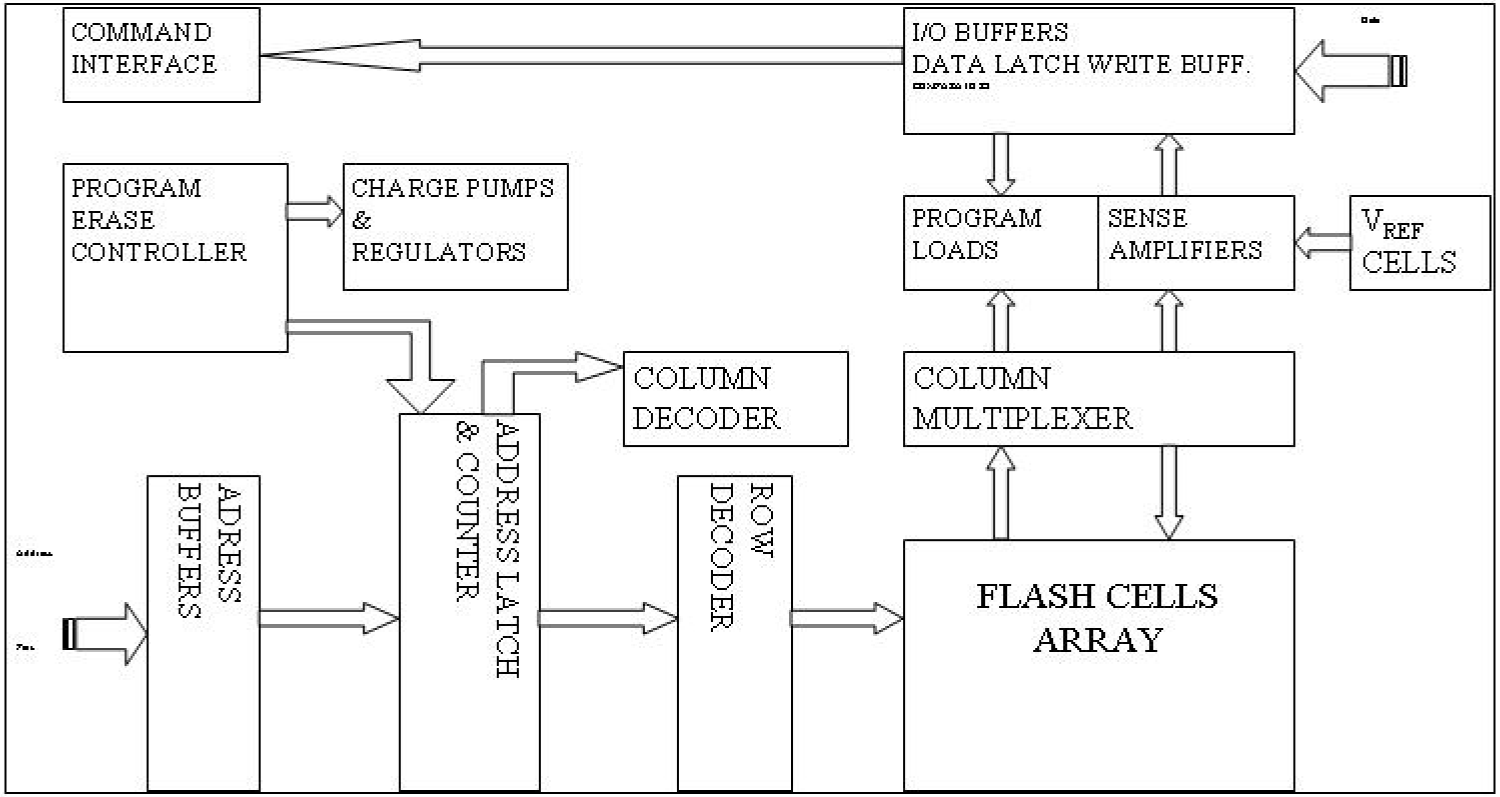
Hierarchical organization

- Read delay is proportional to the row's length ➔ row length must be limited
- Flexibility of erase operation is another parameter that defines memory organization. Erase is carried out in sectors. Sectors are arranged to form an array made up by vertical and horizontal strips, and can be organized by rows and columns
  - Larger sectors ➔ faster erase
  - Smaller sectors ➔ simpler programming and memory management
- The chosen organization affects row and column decoding strategy
- To confine negative effects of gate leakage and stresses, a hierarchical organization is used

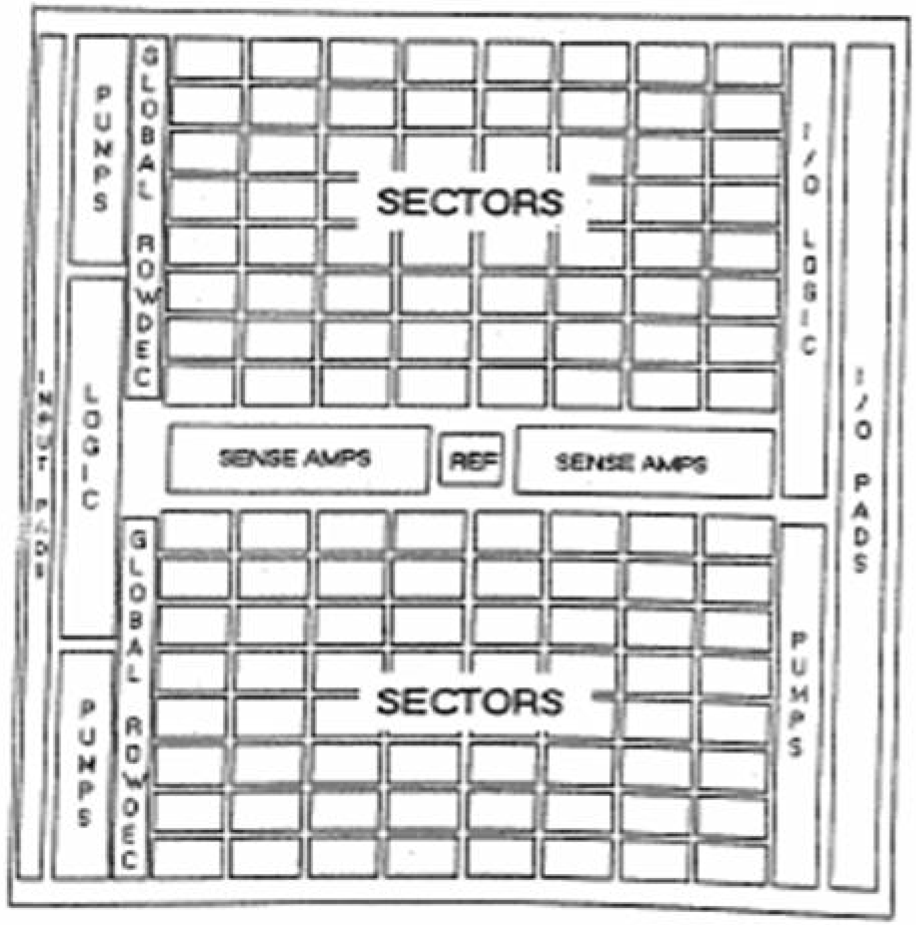


Logic Architecture Inside Flash Device

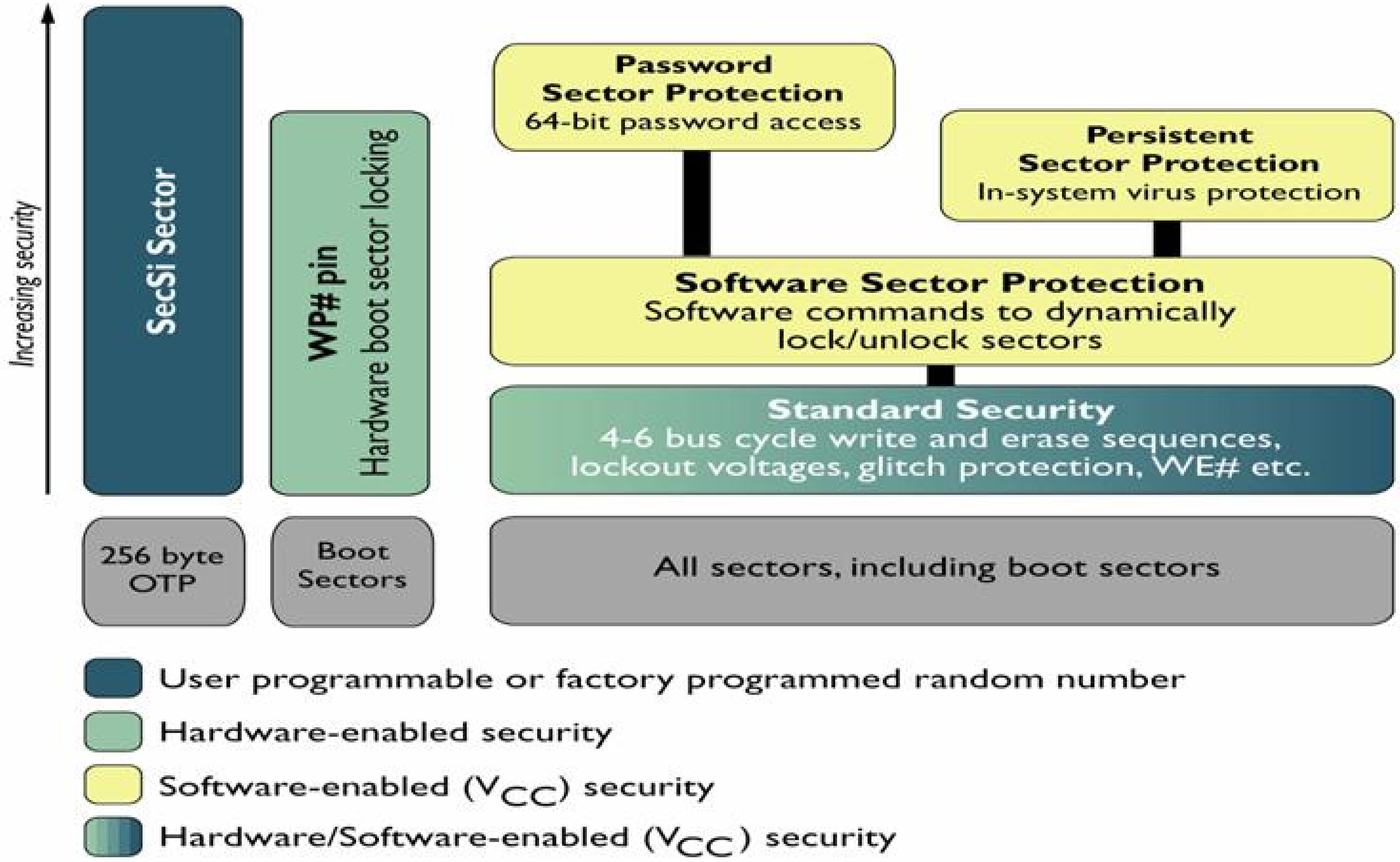
- Large area of a standard flash device is occupied by circuitry devoted to implementing various functions as shown in a simplified NOR device block diagram



High Density Flash Array



Flash Security Features Overview



Increasing security

SecSi Sector

WP# pin
Hardware boot sector locking

Password Sector Protection
64-bit password access

Persistent Sector Protection
In-system virus protection

Software Sector Protection
Software commands to dynamically lock/unlock sectors

Standard Security
4-6 bus cycle write and erase sequences, lockout voltages, glitch protection, WE# etc.

256 byte OTP

Boot Sectors

All sectors, including boot sectors

- 🟦 User programmable or factory programmed random number
- 🟩 Hardware-enabled security
- 🟨 Software-enabled (V_{CC}) security
- ▨ Hardware/Software-enabled (V_{CC}) security

Basic Security Features

- Out-of memory map area used for unique device identification or other security purposes
  - Up to 256 bytes
  - Accessible only by internal FSM
  - One-time programmable by a special (secret) sequence of commands
- Mechanisms protecting from accidental code and data modification
  - No write command is accepted on power-on (noise)
  - The complete control over write operation can be ensured by a special PIN# combination; pins can be protected by packaging
  - No write cycles is accepted when VCC is less than lock-out voltage
  - To protect against glitches, very short pulses (less than 5ns) on pins do not initiate write cycles

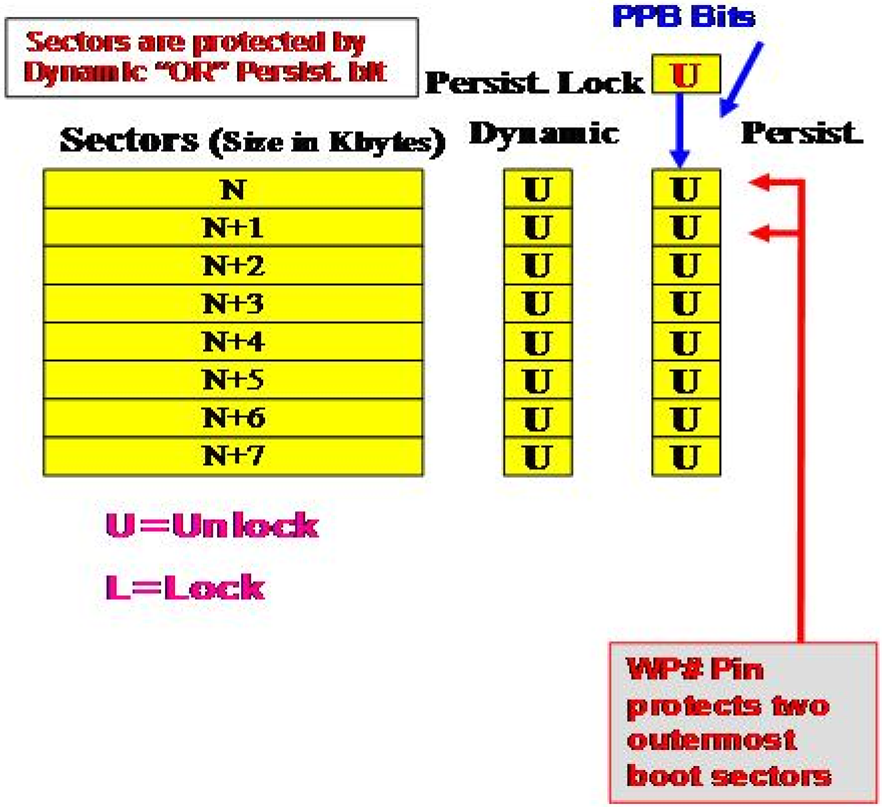
Protection Against Malicious Operations

- HW-based One Time Programmable (OTP) sectors
  - Can be implemented in HW by setting WE# permanently low after the device has been programmed ➔ prevents entire flash from being re-programmed/erased
  - To add flexibility and prevent only some (e.g., boot code storage) sectors from erase/write a special Write Protect Pin (WP#) is used by manufactures to lock out specified sectors by setting WE# permanently low after programming once
- Flexible low-level SW-based OTP
  - A special OTP bit is associated with each sector
    - This bit can only be read by the embedded microcontroller or FSM
    - The OTP protection bits can be only set once by a special (secret) sequence of commands. Once the bit is set, it cannot be unset!
    - When bit is set, the sector can only be read (no access for write/erase operations)

Firmware/SW-based Sector Protection

- To provide better flexibility, the idea of OTP sector protection can be extended in many ways
- Additional re-programmable “soft” protection bit is associated with each sector
  - These bits can be set and re-set only by specially defined (secret) sequence of commands; providing low-level SW-based OTP mechanism
  - After having been set, the chosen combination of soft OTP bits can be “locked” by a special long sequence of commands which cannot be undone, thus “sealing” the access to sectors. This can be done at any stage in a chip life, but only once
- To provide conditional access to otherwise locked sectors, a password-protection mechanism can be implemented
  - A “locked” configuration can be unlocked by presenting a correct (64-128-bit) password. Password is stored outside flash memory address space; password is programmed by a special sequence of commands only once; after having been programmed it is “locked” by the OTP bit. It can be read only by a special command not accessible for applications.

HW & Software Sector Protection



Sectors are protected by Dynamic "OR" Persist. bit

PPB Bits

Persist. Lock U

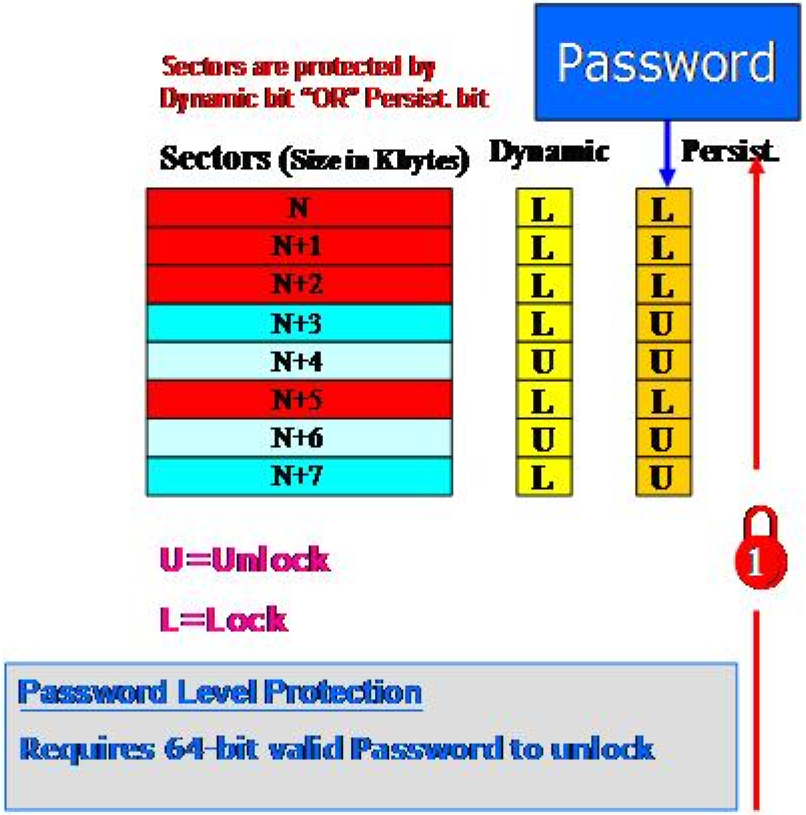
Sectors (Size in Kbytes)	Dynamic	Persist.
N	U	U
N+1	U	U
N+2	U	U
N+3	U	U
N+4	U	U
N+5	U	U
N+6	U	U
N+7	U	U

U=Unlock

L=Lock

WP# Pin protects two outermost boot sectors

Password Sector Protection



Sectors are protected by Dynamic bit "OR" Persist. bit

Sectors (Size in Kbytes)	Dynamic	Persist.
N	L	L
N+1	L	L
N+2	L	L
N+3	L	U
N+4	U	U
N+5	L	L
N+6	U	U
N+7	L	U

U=Unlock

L=Lock

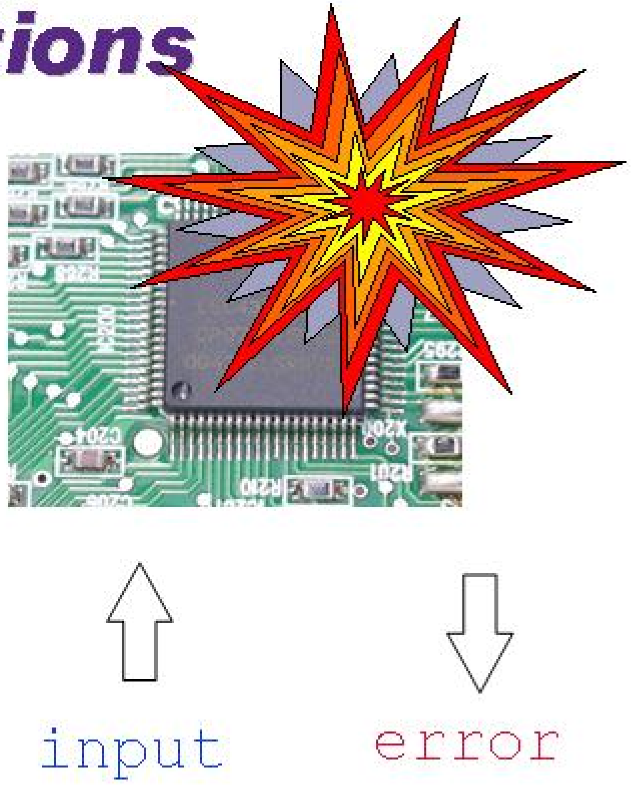
Password Level Protection

Requires 64-bit valid Password to unlock

Fault Generation (stress)

Apply combinations of strange environmental conditions

- **Vcc**
- **Glitch**
- Clock
- **Temperature**
- UV
- **Light**
- X-Rays
- …

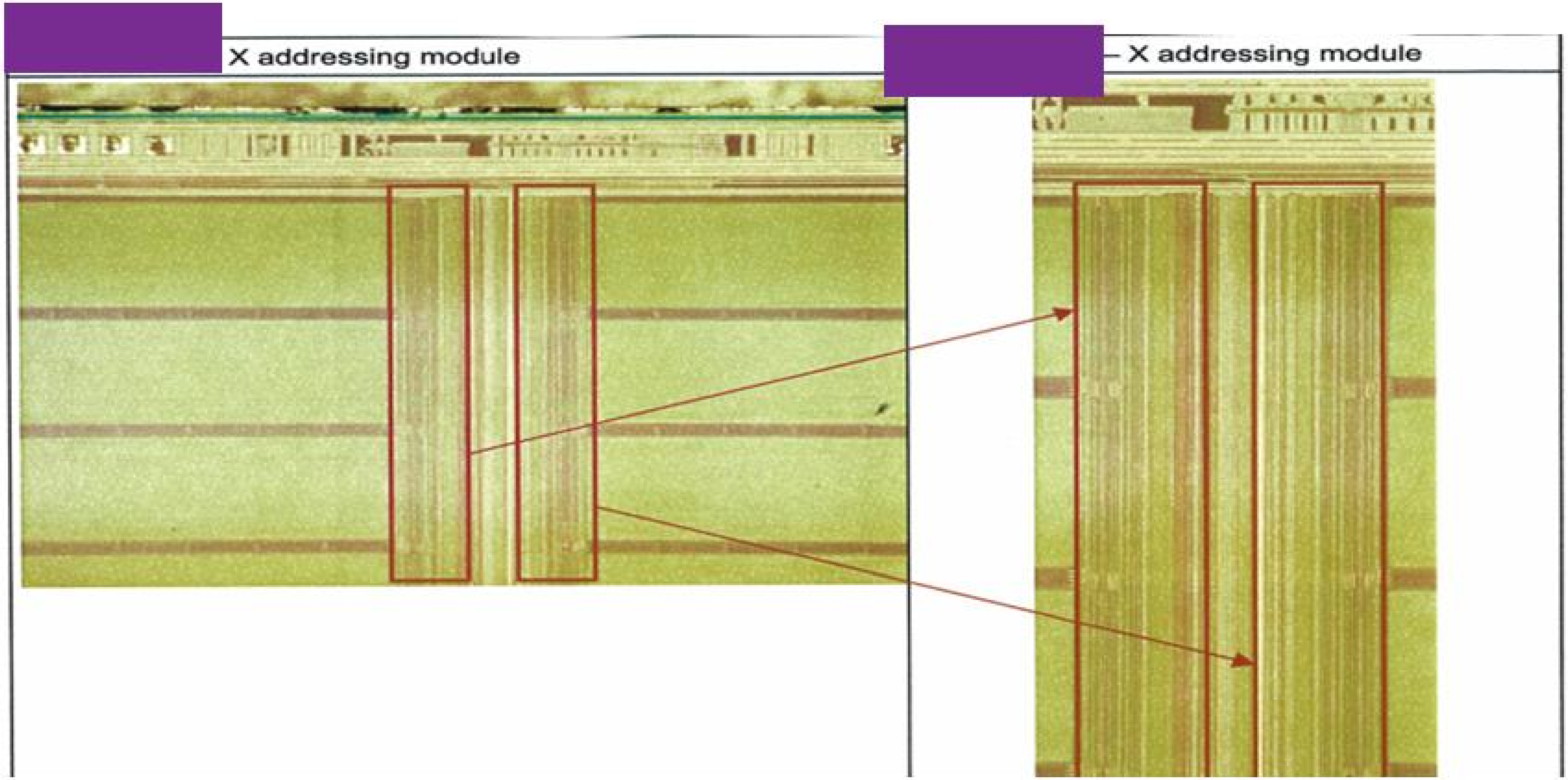

input

error

and bypass or infer secrets

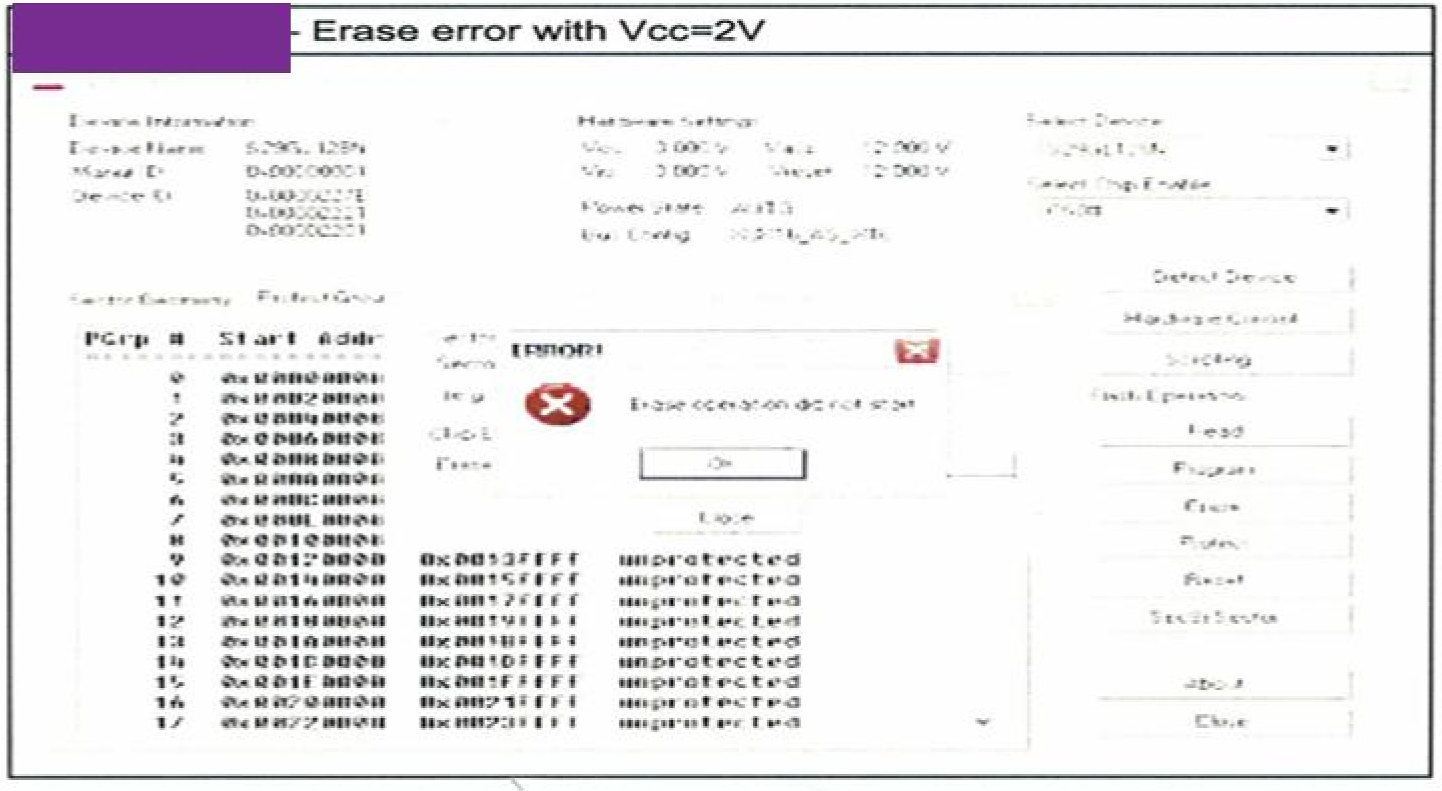
Decapsulation

Although there are 3-4 metal layers, decapsulation is possible



Low Voltage

Write and erase operations are not possible



[redacted] - Erase error with Vcc=2V

Device Information
Device Name S29GL128N
Manuf ID 0x00000001
Device ID 0x0000227E
0x00002221
0x00002201

Hardware Settings
Vcc 3.000 V Vacc 12.000 V
Vio 3.000 V Vhvpe 12.000 V
Power state AUTO
Bus Config X8X16_AS_X16

Select Device S29GL128N
Select Chip Enable CS0

Sector Geometry Protect Group

```
PGrp #   Start Addr
-----------------------
    0    0x00000000
    1    0x00020000
    2    0x00040000
    3    0x00060000
    4    0x00080000
    5    0x000A0000
    6    0x000C0000
    7    0x000E0000
    8    0x00100000
    9    0x00120000   0x0013FFFF   unprotected
   10    0x00140000   0x0015FFFF   unprotected
   11    0x00160000   0x0017FFFF   unprotected
   12    0x00180000   0x0019FFFF   unprotected
   13    0x001A0000   0x001BFFFF   unprotected
   14    0x001C0000   0x001DFFFF   unprotected
   15    0x001E0000   0x001FFFFF   unprotected
   16    0x00200000   0x0021FFFF   unprotected
   17    0x00220000   0x0023FFFF   unprotected
```

ERROR!

Erase operation did not start

High Voltage: Read Operation

Read operation at high voltage results in occasional bit errors

- :200I2000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFDF
- :20014000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFBF

High Voltage: Write Operation

Write operation at high voltage results in correct data being written
However, uncontrolled side-effects are produced
(i.e., other cells are being programmed as well)

- Dump after written pattern with Vcc=5,8V

```
• :200000000I23FFFFFFFFFFFFFFFFF FF F F FF FFFFFFFFFFFFFFFFFFFFFFFFFFFFF F FFFDA
  :20002000FFFF4567FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF32

• :20004000FFFFFFFF89ABFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF8A

• :20006000FFFFFFFFFFFFCDEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE2
  :20008000FFFFFFFFFFFFFFFFO1 23FFFFFFFFFFFFFFFFFFFFFFFFFFFF9FFFFFFFFFFFFFFF9A
  :2000A000FFFFFFFFFFFFFFFFFFFF4S67FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFB2

• :2000C000FFFFFFFFFFFFFFFFFFFFFFFF89ABFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFOA
  :2000E000FFFFFFFFFFFFFFFFFFFFFFFFFFFFCDEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF62
  :20010000BFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFOI2SFFFFFFFFFFFFFFFFFFFFFFFFFFFF1 9
  20012000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF4567FFFFFFFFFFFFFFFFFFFFFFFF31

• :20014000FFFFFFFF9DBFFFFFFFFFFFFFFFFFFFFFFFFFFFFF89ABFFFFFFFFFFFFFFFFFFFF2B
  :200I6000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFCDEFFFFFFFFFFFFFFFFFE1
```

High Voltage: Erase Operation

Erase operation is successful

However some bits may remain non-erased

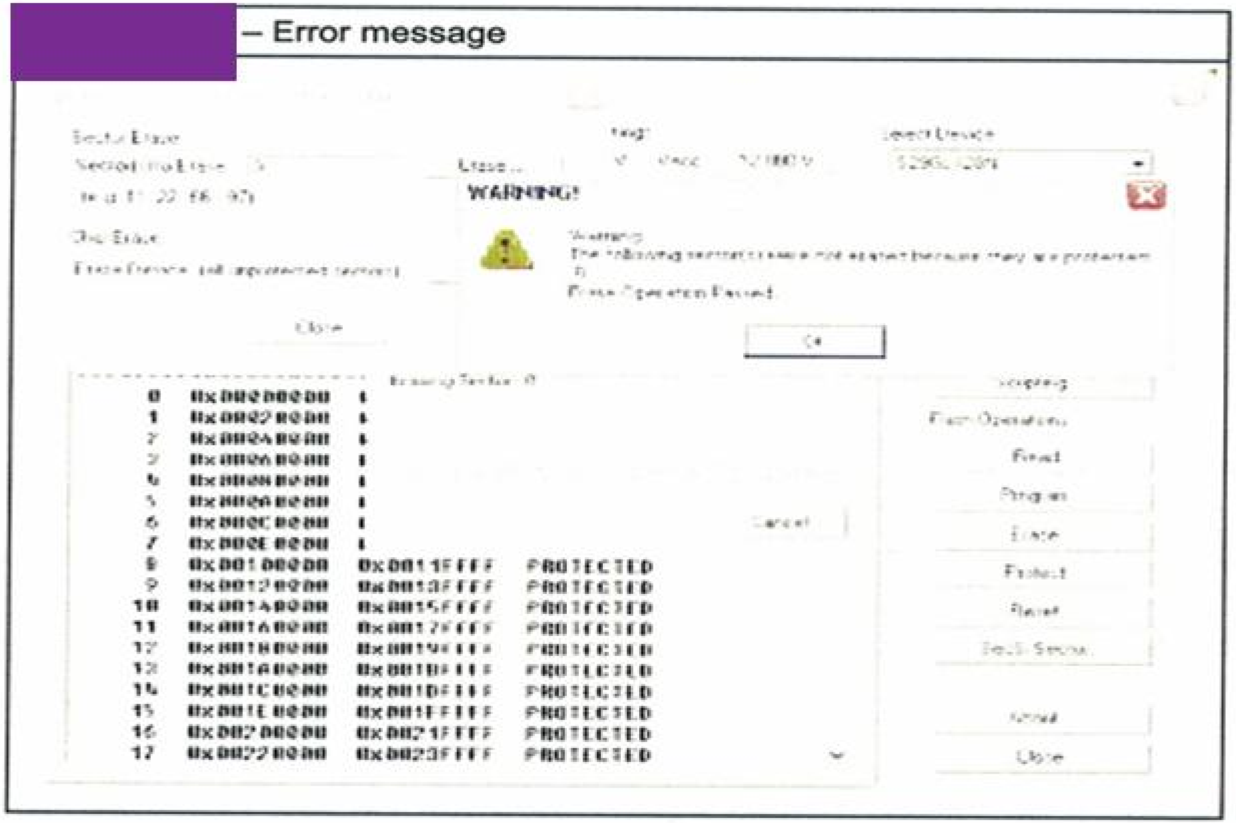
- Dump after erase with Vcc 5,8V
- :20022000FFFFFFFFFFFFFFFFFFFFFFFFEFEFFFFFEFEFFFEFFFFFFFFFEFFFFFFFFFFFFFFFDE
- 20024000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFBE
- :20026000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF9E
- :20028000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE
- :2002A000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF5E

High V: Erasing Protected Sector

Sector protection mechanism is robust

Attempt to erase protected sector results in error message

– Error message



WARNING!

Warning:
[illegible]
Erase Operation Passed.

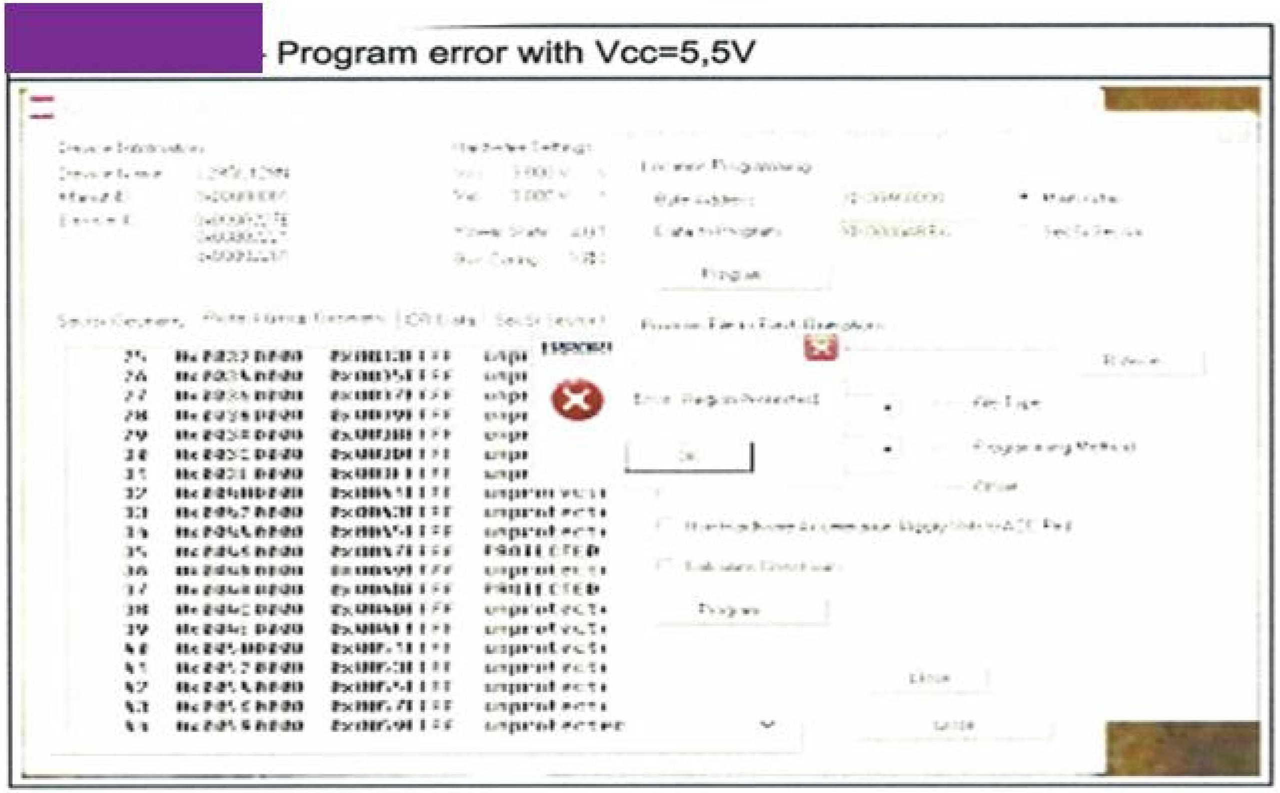
Erasing Sector: 0

```
 0   0x00000000   1
 1   0x00020000   1
 2   0x00040000   1
 3   0x00060000   1
 4   0x00080000   1
 5   0x000A0000   1
 6   0x000C0000   1
 7   0x000E0000   1
 8   0x00100000   0x0011FFFF   PROTECTED
 9   0x00120000   0x0013FFFF   PROTECTED
10   0x00140000   0x0015FFFF   PROTECTED
11   0x00160000   0x0017FFFF   PROTECTED
12   0x00180000   0x0019FFFF   PROTECTED
13   0x001A0000   0x001BFFFF   PROTECTED
14   0x001C0000   0x001DFFFF   PROTECTED
15   0x001E0000   0x001FFFFF   PROTECTED
16   0x00200000   0x0021FFFF   PROTECTED
17   0x00220000   0x0023FFFF   PROTECTED
```

High V - Programming Protected Sector

- Sector protection mechanism is robust: attempt to write into a protected sector results in error message; no write is performed

[redacted] - Program error with Vcc=5,5V



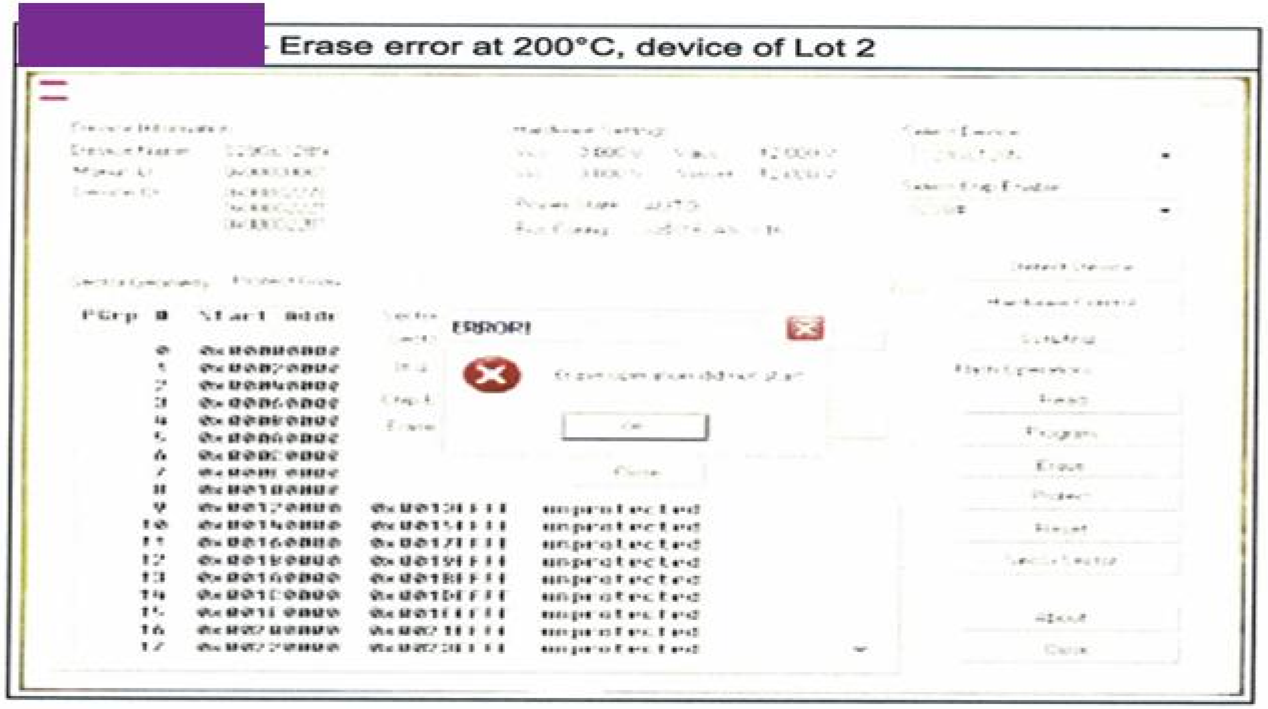
```
25   [illegible]   [illegible]   unpr
26   [illegible]   [illegible]   unpr
27   [illegible]   [illegible]   unpr
28   [illegible]   [illegible]   unpr
29   [illegible]   [illegible]   unpr
30   [illegible]   [illegible]   unpr
31   [illegible]   [illegible]   unpr
32   [illegible]   [illegible]   unprotected
33   [illegible]   [illegible]   unprotected
34   [illegible]   [illegible]   unprotected
35   [illegible]   [illegible]   PROTECTED
36   [illegible]   [illegible]   unprotected
37   [illegible]   [illegible]   PROTECTED
38   [illegible]   [illegible]   unprotected
39   [illegible]   [illegible]   unprotected
40   [illegible]   [illegible]   unprotected
41   [illegible]   [illegible]   unprotected
42   [illegible]   [illegible]   unprotected
43   [illegible]   [illegible]   unprotected
44   [illegible]   [illegible]   unprotected
```

Error: Region Protected

Erase Protected Sector: High Temperature

Nor flash is resistant to temperature up to 200 C; afterwards attempts to execute operations result in error message and flash becomes un-operational

[redacted] - Erase error at 200°C, device of Lot 2



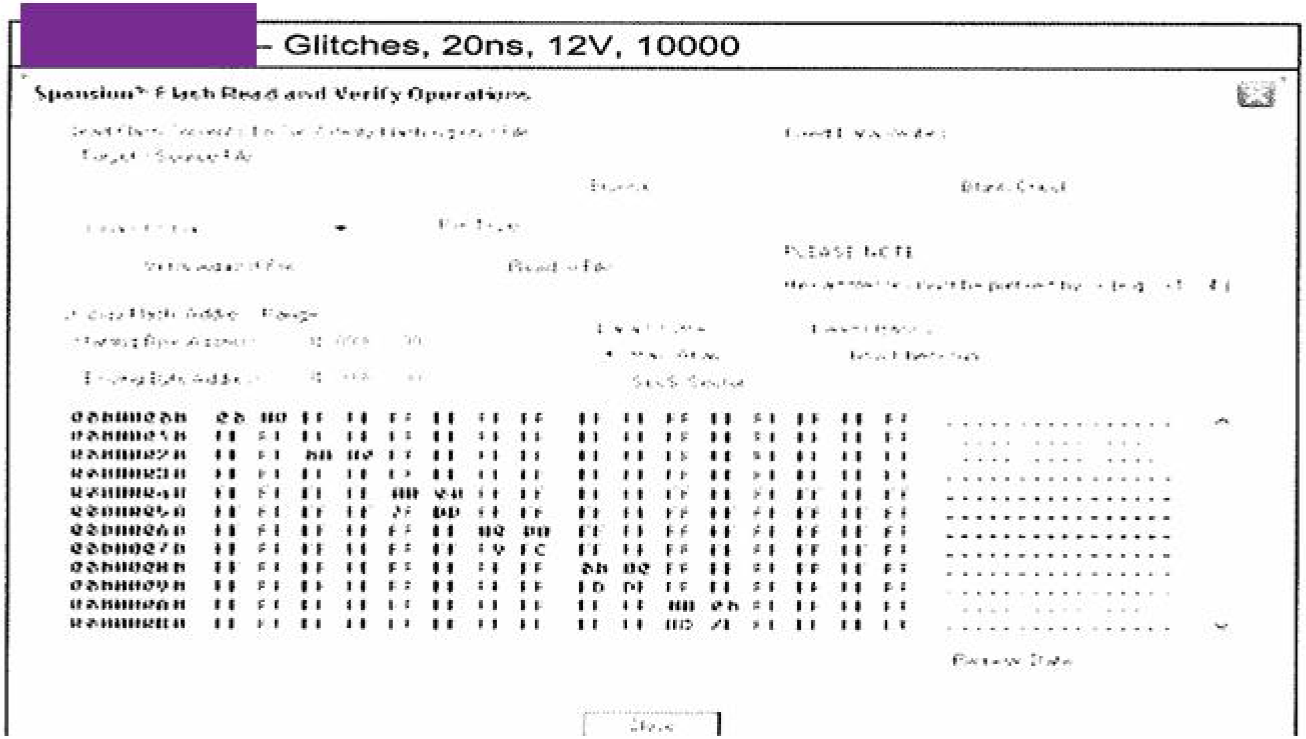
ERROR!

[illegible]

PGrp #	Start addr		
0	0x00000000		
1	0x00020000		
2	0x00040000		
3	0x00060000		
4	0x00080000		
5	0x000A0000		
6	0x000C0000		
7	0x000E0000		
8	0x00100000		
9	0x00120000	0x0013FFFF	unprotected
10	0x00140000	0x0015FFFF	unprotected
11	0x00160000	0x0017FFFF	unprotected
12	0x00180000	0x0019FFFF	unprotected
13	0x001A0000	0x001BFFFF	unprotected
14	0x001C0000	0x001DFFFF	unprotected
15	0x001E0000	0x001FFFFF	unprotected
16	0x00200000	0x0021FFFF	unprotected
17	0x00220000	0x0023FFFF	unprotected

Glitches: Read Operation

- Glitches up to 20 ns have no effect on read operation
- Glitches 20 ns introduce errors
- The higher the voltage the more memory corruption
- Errors may be detected with error detection mechansism



[redacted] – Glitches, 20ns, 12V, 10000

Spansion™ Flash Read and Verify Operations

PLEASE NOTE

Glitches: Write Operation

- Short glitches have no effect on write operations
- Glitches 100 ns may result in occasional uncontrolled bit error
- Glitches 150 ns result in aborting write operation and error message
- Glitches during write operation on sector protection bits result in error message. However, some unpredictable side-effects arise (e.g., while operation is reported aborted, the protection bit is still set)

Light Attacks

Laser light attacks are more dangerous when light is focused on address decoders, FSM's, voltage regulators, etc. rather than on memory cells array

Picture n° 64 – Laser, Reading, sensitive areas

[redacted]

[redacted]

Laser Attack: Read Operation

While it was possible to corrupt data during read operation, EDC mechanism is capable of detecting errors

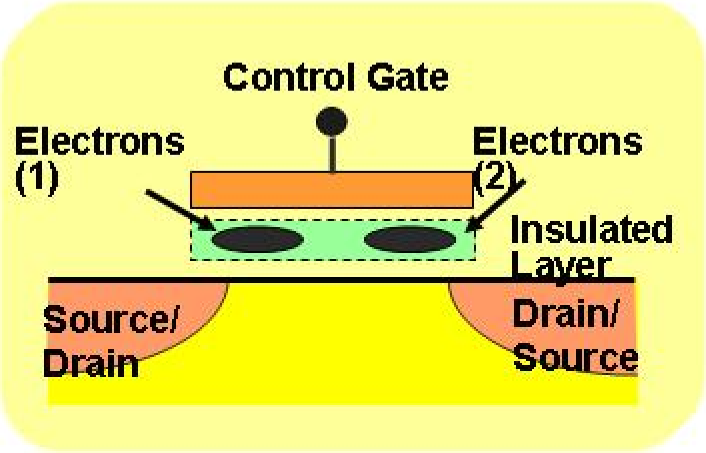
Laser Attack: Write Operation

- The results of laser attacks during write operation are very mixed
- Depending on the spot where light has been flashed, the consequences can be either:
  - None (operation is performed correctly)
  - Data could be written to another (but similar) address
- To write data in a slightly more controlled way, one needs to know exact device configuration, glue logic, addressing scheme, internal details of implementation of write operation and one must induce a very "strong" error (long duration)
- Some devices in the same series are more resistant to laser attacks during write operation

MirrorBit Flash Memory for Smart Cards

- Latest Flash Technology for Smart Cards
  - 2 bits per cell
  - 90 nm MirrorBit™ Technology
  - next generations: 65 nm and 45 nm
- Submitted to evaluation lab
- Invasive attacks *much more difficult* on such small technology
- Far *less error prone* when stressed (FA)
- *More resources required* for successful invasive attacks

MirrorBit



Traps electrons on two sides of the insulated layer (2bit/cell)

Systems on Flash: High Density Cards

- Next Generation Smart Cards
- High Density cards
  - MegaBytes of Flash memory
  - User data in (OR)NAND Flash (16, 64, 256 MB and more)
  - NO ROM, NO EEPROM
  - Operating system in CodeFlash (512 KB of NOR Flash)
  - Application data and keys in Emulated EEPROM (128, 256 KB NOR Flash)
  - RAM (24, 48, 64 KB)
  - **All this on a Single Die** (75mm^2)
  - MMC and USB high speed interfaces
  - On-the-fly encryption of ORNAND Flash

Thank you !

Elena.Trichina@spansion.com

SPANSION™

Trademark Attribution

Spansion, the Spansion Logo and combinations thereof are trademarks of Spansion LLC. Other product names used in this presentation are for identification purposes only and may be trademarks of their respective companies.