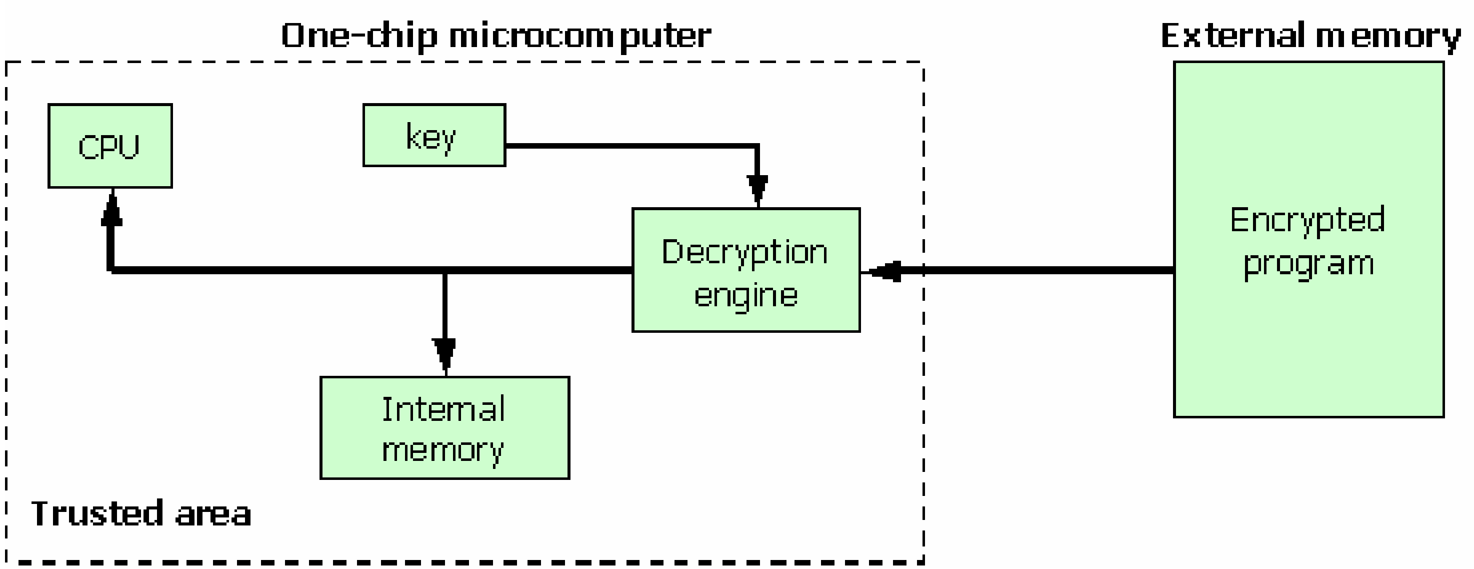
Countermeasures

- Bus Encryption
- Top-layer Sensor Meshes
- ASICs and custom ICs
- Internal Voltage and Clock Frequency Sensors
- Light Sensor

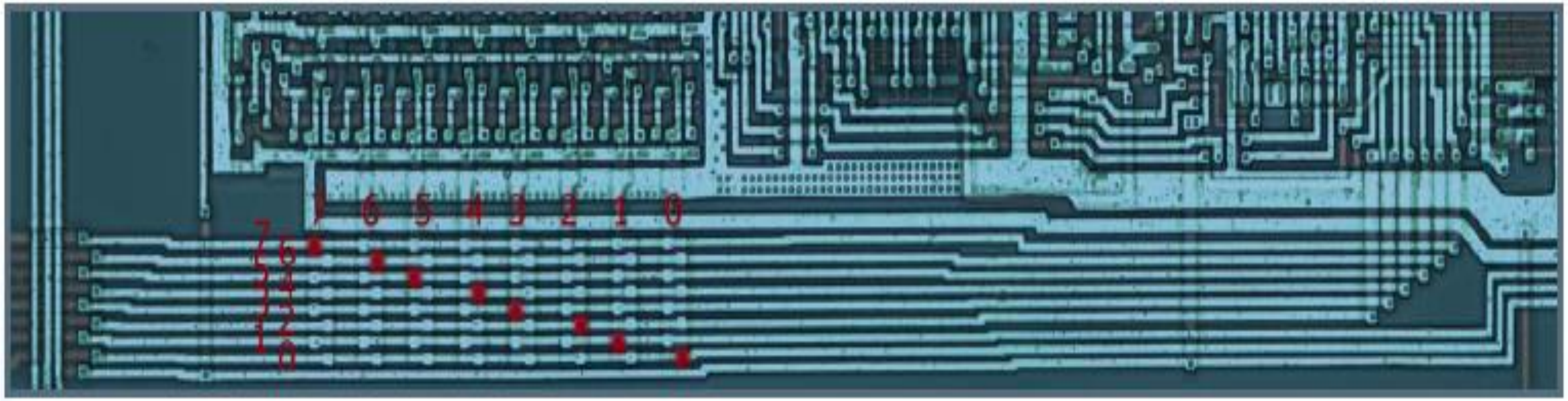
Countermeasures: Bus Encryption

- The **bus encryption** is used to protect the sensitive information from probing
  - Basically, the memory content is encrypted and then sent to the CPU by data bus
  - Before the data used in CPU, it is decrypted



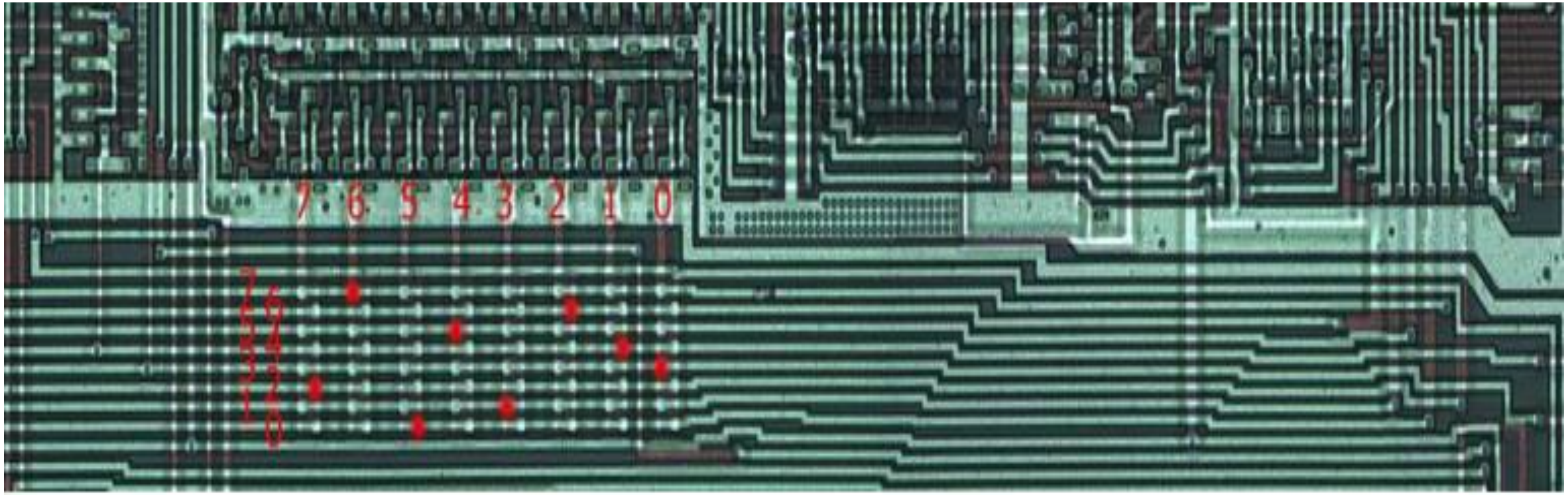
Countermeasure: Bus Scrambling

- **Typical probing areas**
  - Memory bus drivers
  - Data bus itself where lines are organized in proper CPU bus width
  - Bus order is always in order (0..7 or 7..0)



Countermeasure: Bus Scrambling

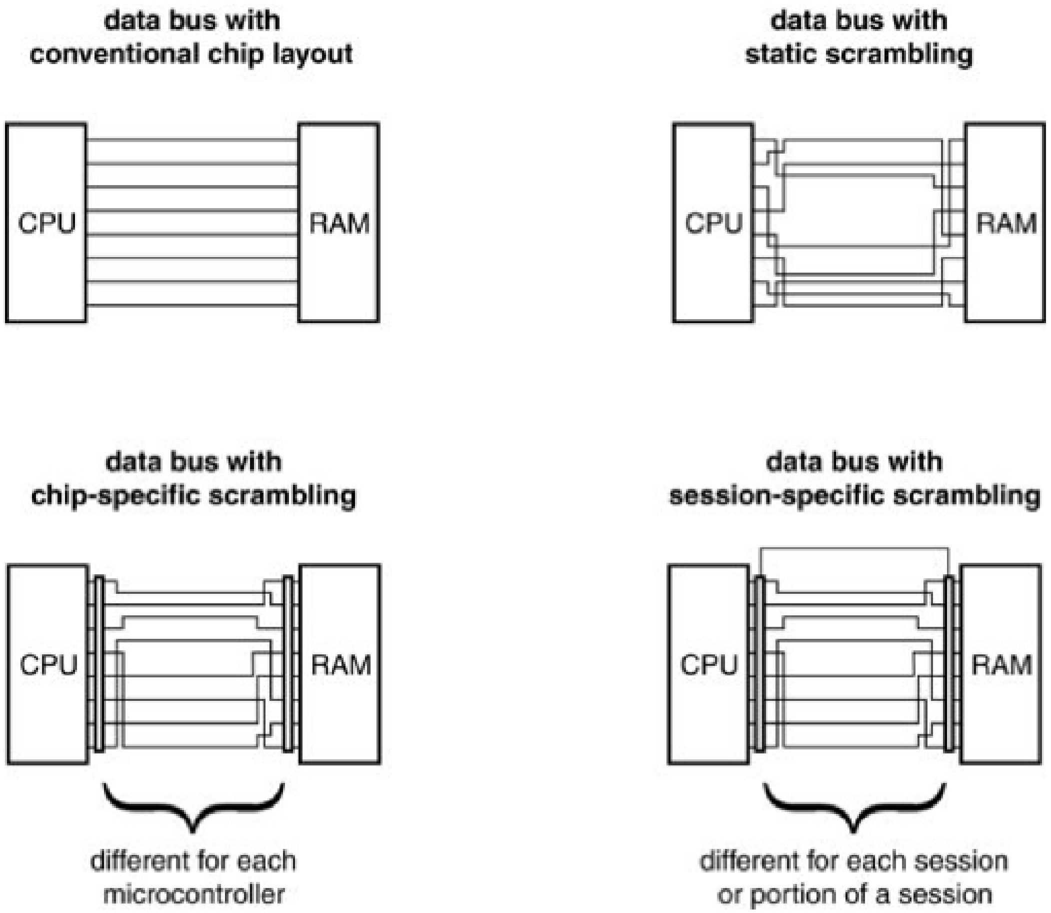
- **Data bus scrambling is used to confuse attackers**
  - Order of the data bus is changed to make it difficult to observe bus signals



Many smart cards have scrambled internal memory bus.
they are arranged randomly and swapped several times or even placed top of each other in different layers.

Bus Scrambling

- Bus scrambling was originally performed as static. Memory buses for each chip scrambled in the same scrambling scheme. In this way, it is not difficult for an attacker to find scrambling order of the chip. When the adversary find the order for one chip he can use it for all them.
- To improve the protection that is offered by scrambling can be improved by using chip-specific scrambling. To implement this, there is no need to create different masks for each chip. Only randomizer circuit is needed to achieve chip-specific scrambling. Scrambling order can be changed depending on chip serial number or unique another feature.
- Like chip-specific scrambling, session specific scrambling also can be used to increase the security of the device.



Countermeasures: Sensors

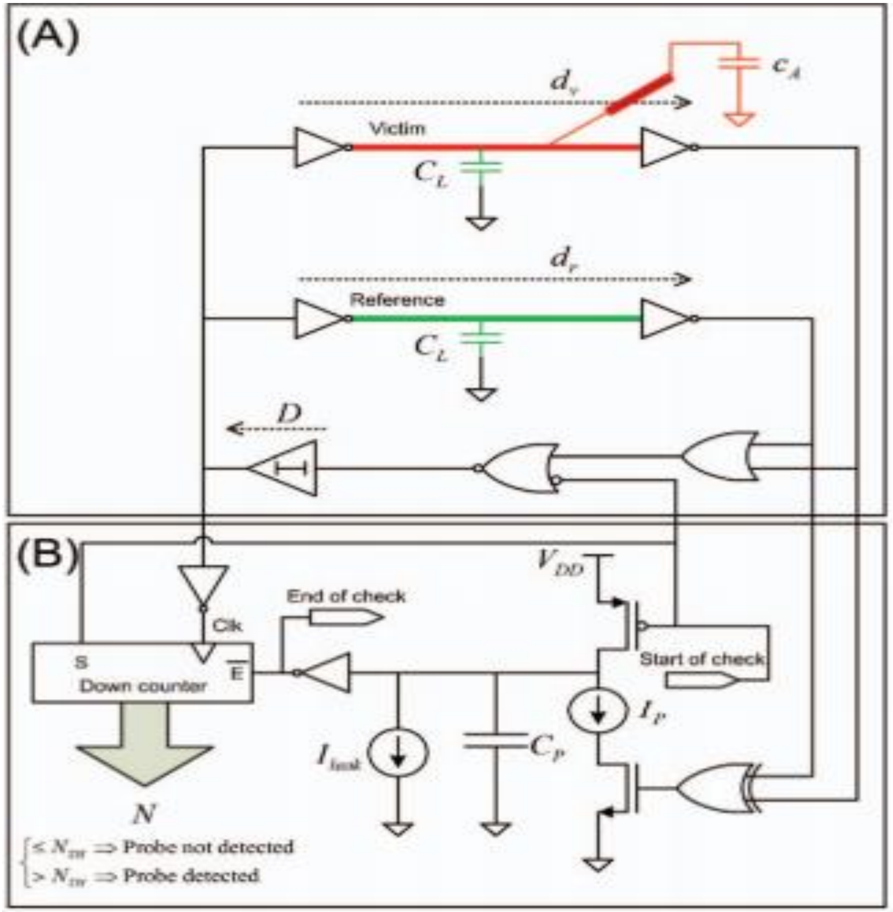
- Different kind of sensors can be used to detect attack attempt
    - Voltage and frequency sensors for glitching attacks
    - Light sensor can be helpful against decapsulation of the device

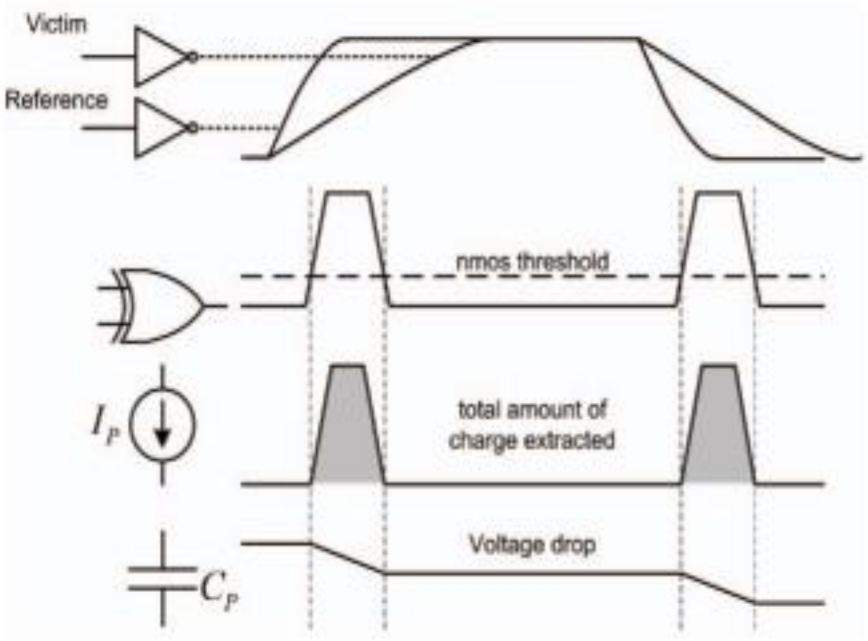
- Special purpose sensors can be created to detect probing
    - Ring oscillator based detector (Probing Attempt Detector)

Sensors: Probing Attempt Detector (PAD)

- Exploits the fact that probing will change the capacitance in the bus line.
  - Place ring oscillators on the bus lines
  - When the probe touches the one or more bus lines, frequency of the ring oscillator changes
    - Because of the added capacitance
  - PAD observes the bus lines continuously, when they have significant difference, it sets a flag that there is a probing attempt on one of the lines

Sensors: Probing Attempt Detector





Sensors: Probing Attempt Detector

- The Sensor consists of two parts, one is the ring oscillator part and the other is detector part.
- Without any probing attempts, two ring oscillator will have the same frequency.
- When a probe touches the one of the lines, two pulses in each cycle is produced at the output of the xor gate.
- These pulses will discharge the capacitance in the detector.
- At the same time counter is counting down, when the voltage of the capacitance reaches below threshold voltage of the inverter, counter will stop.
- If the value of the counter has a value below the predetermined threshold value, there is not probe, if the value is greater than theshold value, there is a probing attempt on one of the lines.