Security Challenges for High Density Smart Cards

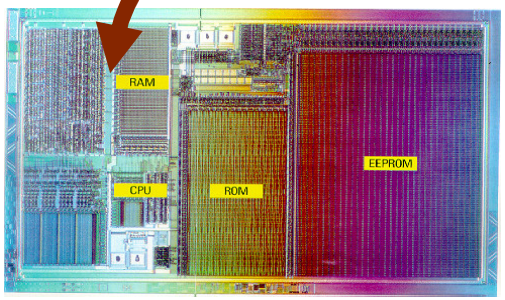
Dr. Helena Handschuh

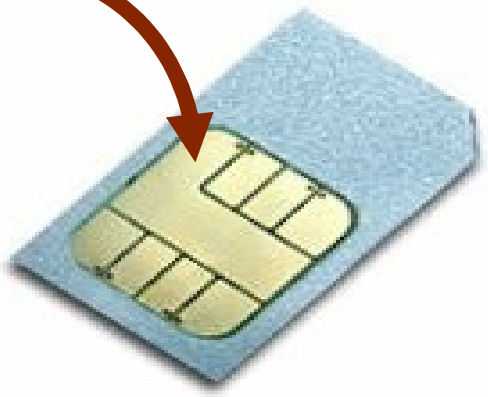
Spansion EMEA

What is a traditional Smart Card?

SPANSION™

A piece of silicon and a plastic body





Contains:

- millions of transistors
- RAM, ROM, EEPROM, FLASH and a CPU
- HW Crypto-coprocessors (DES, AES, RSA, DSA, ECC)

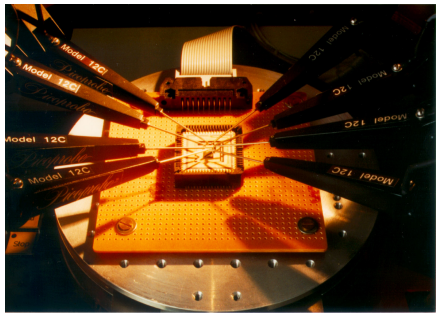
Applications: SIM cards, Credit Cards, Electronic Passport

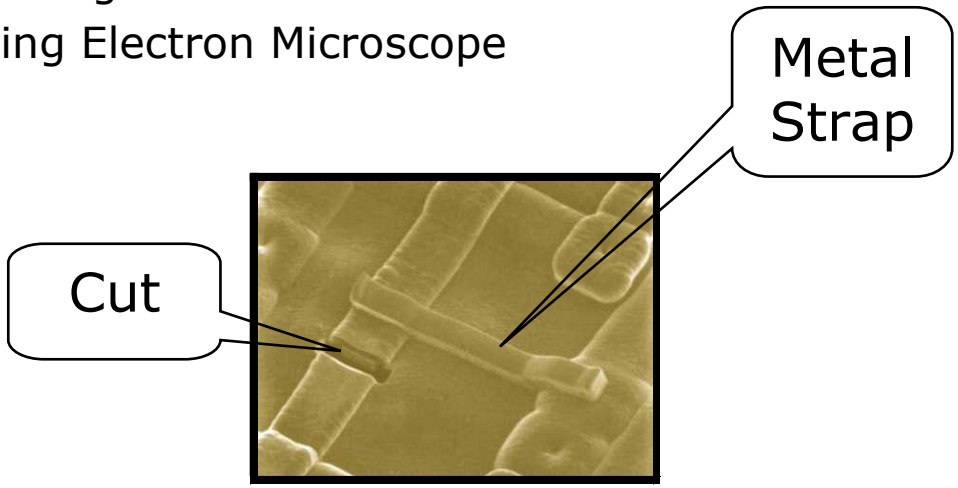
High Density vs Typical Smart Cards: Flash takes over…

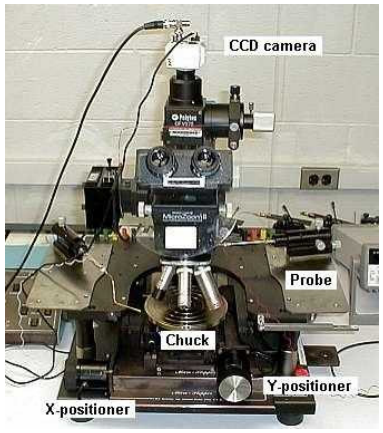
	Typical	***High Density***
Confidential Operating system	ROM (512 KB)	CodeFlash (512 KB NOR Flash)
Application Data, Secret Keys	EEPROM (256 KB)	Emulated EEPROM (128 KB NOR FLASH)
RAM	5 KB	24, 48, 64 KB
User Data	In EEPROM	4 to 256 MB (OR)NAND FLASH
Interface	ISO 9600 bit/s	+ USB, MMC High-speed protocols
Die Size	25 mm^2 in 0,13µm technology	75 mm^2 in 90nm technology

Hardware Attacks : observing memory bits and buses

- Nanotechnologies will inherit typical invasive and semi-invasive attacks on Smart Cards
  - Chemical and Mechanical Etching
  - Decapsulation
  - Probing
  - Fibbing
  - De-layering
  - Scanning Electron Microscope





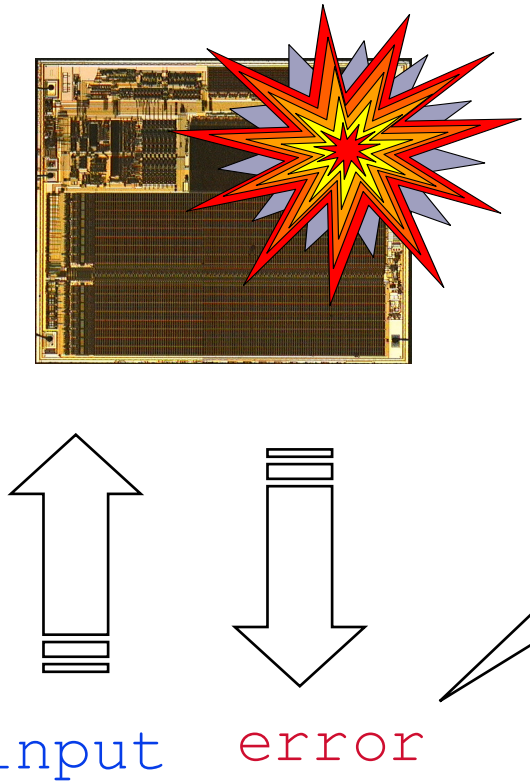


Fault Generation and Differential Fault Attacks

SPANSION™

Out-of-range environmental conditions allow to bypass or infer secrets

- Vcc
- Glitch
- Clock
- Temperature
- UV
- Light Flashes
- X-Rays
- Lasers
- ...



High Density Flash Memory for Smart Cards

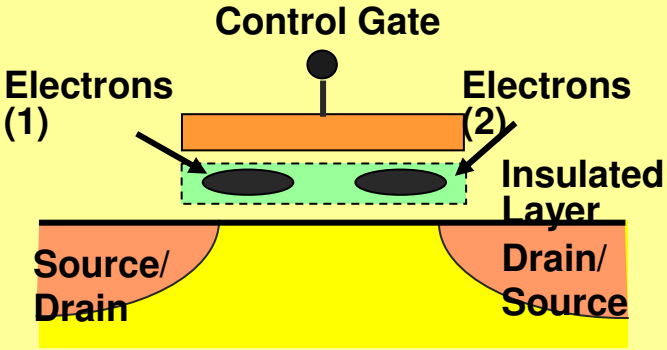
- Current Flash Technology for Smart Cards
  - 90 nm MirrorBit™ Technology
  - next generations: 65 nm, 45 nm, 32 nm

- Submitted to evaluation lab :

MirrorBit™

- Invasive attacks *much more difficult* on such small technology than on EEPROM, ROM
- Far *less error prone* when stressed (fault attacks).
- *More resources required* (time, knowledge, high precision tools) for successful invasive attacks.

- *But this may change over time ...*



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

Hardware Security Measures adapted from Secure Smart Card Design

- Security Sensors

  (VCC, Temp, Light, UV, Clock, glitches)

- Shrinking technology scale

- Several Metal Layers
- Conductive metal shield
- Hand-routing of sensitive lines
- Deeply buried buses
- Glue Logic
- Current scramblers

- NOR FLASH Memory Scrambling:
  - Data scrambling
  - Address scrambling

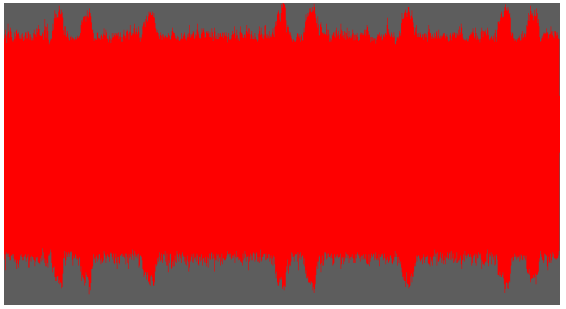
- Generally a somewhat light encryption algorithm
- Has to be transparent in the architecture
- A few gates only, no delay but high security required (!)

New Security Challenges for Next generation High Density Cards

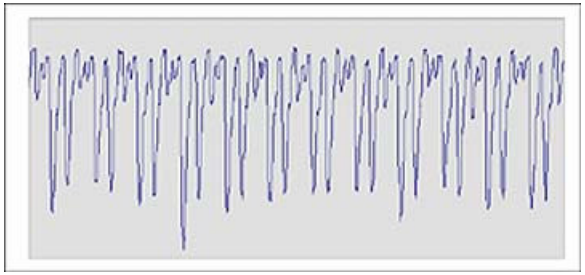
- On-the-fly encryption of Megabytes of data
  - high throughput encryption cores (3-5 Mbyte/s)
  - transparent for the user (as fast as USB/MMC protocols)
  - need to work in low power USIM mode too (below 10 mA)
- *Integrate everything on a Single Die*
  - Dual die solutions have an intrinsic security weakness (bus)
- Secure personalisation process for Flash
  - no more ROM for the sensitive operating system and algos
  - Initial Program Loader with Public Key capabilities required
  - highly secure memory scrambling is mandatory
- Security for One-Time-Programmable Flash sectors ?
- Secure Boot from CodeFlash

Side-Channel Attacks on Cryptographic Hardware: Physical properties leak information

- Typical side-channels:
  - power consumption
  - timing information
  - electromagnetic radiation
  - radio-frequency analysis (Contactless, RFID)



- Information leakage:
  - depends on secret keys
  - can be measured
  - can be cryptanalysed by statistical methods

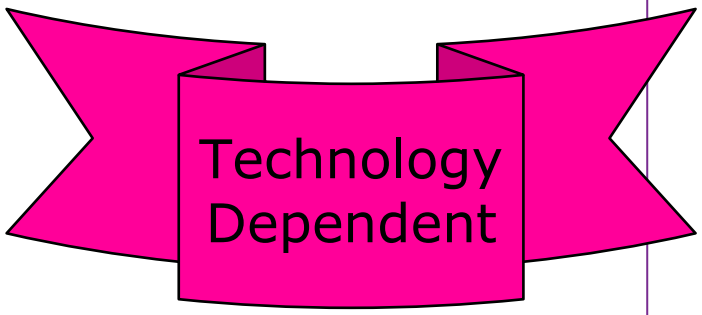


- *A few hundreds of power curves allow to retrieve cryptographic keys*

Countermeasures for Secret Key Algorithms (AES, DES)

- Need to be built-in at design-level (not add-on such as for RSA)
  - clock jitter or random desynchronization
  - increase noise to signal ratio
    - by random register pre-charging,
    - random operation interleaving, ...
  - masking intermediate data
    - multiplicative masking
    - masking at the gate level
  - equalize power dissipation: dual-rail logic, non-standard logic, requires full custom design

- Use additional hardware security features
  - current scramblers
  - noise generators



Side-channel attacks in the real world... There is still hope!

- Very difficult to obtain open access to devices to set-up template attacks
- Many concurrent countermeasures
- Hardware attacks mostly successful on open dedicated designs for evaluation purposes
  - Real attacks on fielded hardware still rare
  - ***More and more difficult as technology shrinks***
- CC: White-box analysis attacks compared to blackbox attacks in the field
- **Smart cards are not the only link in the security chain:**
  - back-end fraud detection systems
- **Security level is a trade-off**
  - as long as cost of fraud < cost of additional security measures, the issuer won't invest
  - Industry accepts a certain level of risk/cost

Conclusion

- Memory and Hardware Crypto cores are vulnerable to physical and side-channel attacks
  - Requires quite some skills for built-in security features
  - But: already many hardware security features available: ***transpose to nanotechnologies***
- ***As technology shrinks, attacks get more difficult***
- High Density concept for Smart Cards introduces new security challenges
- Security Features are always tested by evaluation labs
- Fine balance between security and cost

Helena.Handschuh@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.