Silicon Development for crypto

CROSSBAR

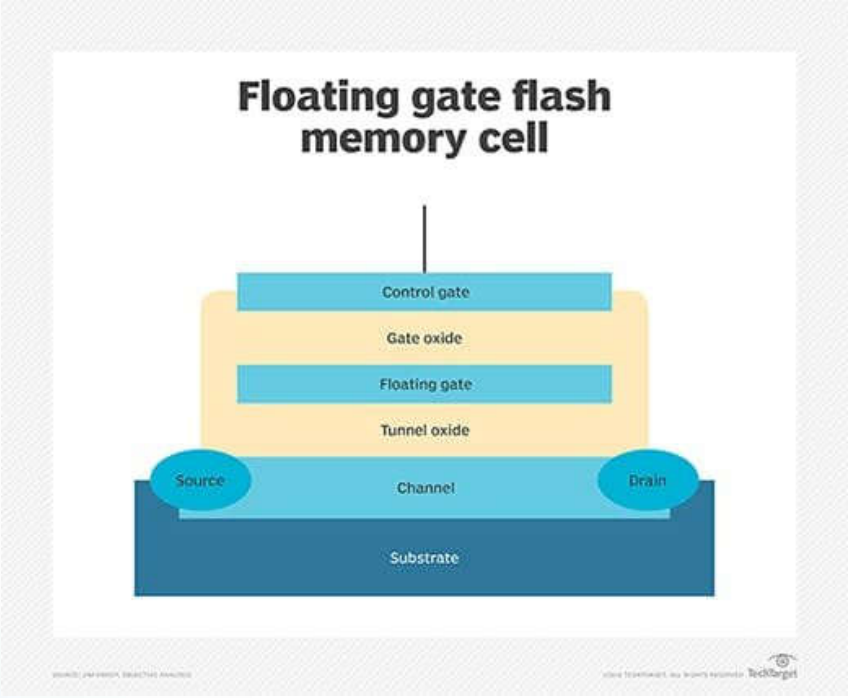
Intersection of Cultures

Crypto culture	Semiconductor culture
Shorter Timelines	Longer Timelines
Start and fix it on the way	Maximum validation before buying masks
Little to no tooling	High fixed tooling (masks, IP, test, qual)
Cost to acquire customer is key metric	Gross margin is key metric
Point solution, focused narrowly	Single chip, multi purpose
Can build value gradually	Quantized : 1 chip is a major undertaking.

- Crypto players might not care about adjacent semiconductor markets
  - However, unless chip requirements are harmonized across the largest possible TAM, good semiconductor support for crypto will not exist.

Aside on memory

- The established way of embedding NV memory with logic is to use floating gate flash.
  - A volume of stored charge influences the underlying channel
  - This approach stops working around 28nm
  - This leads to a field of new technologies broadly called “emerging memories”
  - Emerging memories include various types of Resistive RAMs (RRAMs) and Magnetic RAMs (MRAMs)



- Crossbar is a leader in RRAM

Aside on memory (2)

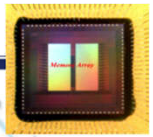
	Flash (trapped charge)	ReRAM
Security	Charge easily readable by microscopy	Highly immune to physical attack
Permanence	Charge continuously leaks; unreliable and short-lived	Metal-based, >100yrs at room temperature
Integration	Cannot be integrated with advanced logic	Can be integrated with advanced logic

Reverse engineering Flash EEPROM memories using Scanning Electron Microscopy

Franck Courbon[1], Sergei Skorobogatov[1], and Christopher Woods[2]

[1] Computer Laboratory, University of Cambridge
[2] Quo Vadis Labs, London, UK

Abstract. In this article, a methodology to extract Flash EEPROM memory contents is presented. Samples are first backside prepared to expose the tunnel oxide of floating gate transistors. Then, a Scanning Electron Microscope (SEM) in the so called Passive Voltage Contrast



Conclusion

During the extensive delayering operation, it appears that some evidence of charging and possible physical "rivets" were observed during the direct read of the memory array, particularly in the upper layers of the memory stack just below the Ag/Si composite material. However, the charging and "rivets" did not appear to have a systematic programming pattern, and for the most part were random.

Backside attacks were unsuccessful, likely the consequence of the memory element not being in close to silicon. Backside attempts were made using the state of the art "X-mill" polisher, Focused Ion Beam. Inspection done using EBIC (Electron Beam Induced Current), along with passive voltage contrast imaging did not reveal the state of the RRAM.

At this stage, it appears we were unsuccessful at performing a direct read of the memory array. Review of the report, and feedback from the customer will determine if the charging / "rivet" evidence was significant to the state of the memory cells, and if our RE work at understanding the operation of the memory cell was correct.

Observations on typical wallet

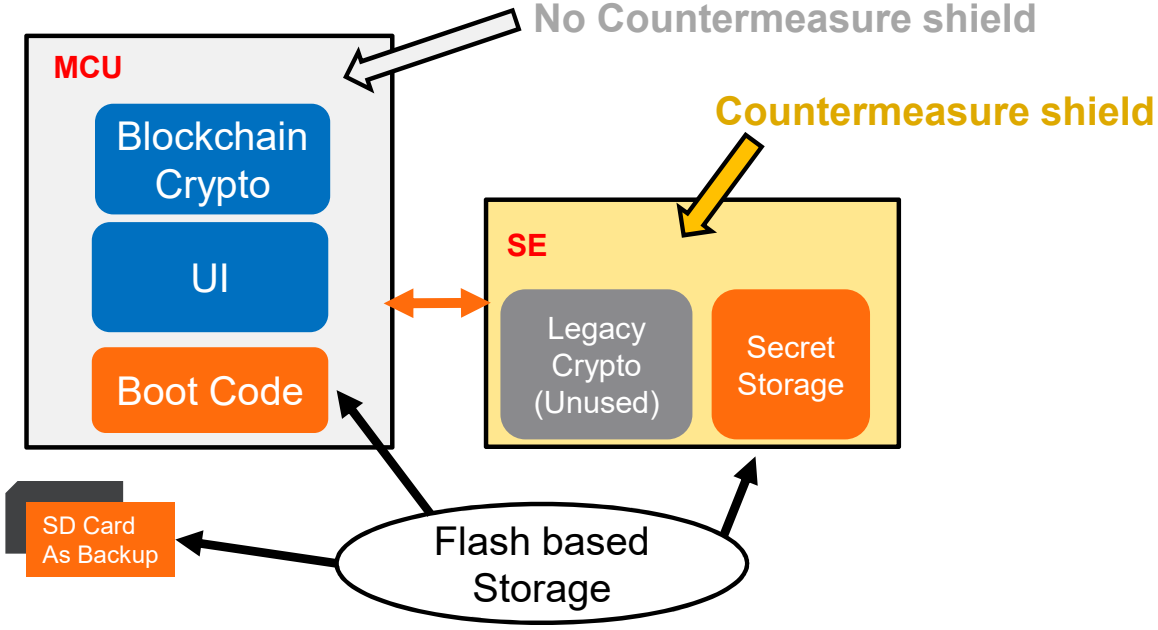
Wallets use the following architecture:

MCU borrowed from consumer market
- Not shielded
- Speed limited by inclusion of Flash

+

SE borrowed from card/SIM market
- Shielded, but….
- Little to no MCU capability
- No peripherals (6-8 pins total)
- Inapplicable crypto from banking and cellular
- Hard to go beyond black-box(*)

Problems with this architecture:
- Crypto, Boot, and UI all execute in non-secure environment.
- Flash memory everywhere (readable, perishable)
- Exposed bus between chips
- Limited UI performance (due to 40nm+)
- SE mostly just a “secure memory”
- No devkit access to SE; inflexible compared to MCU.



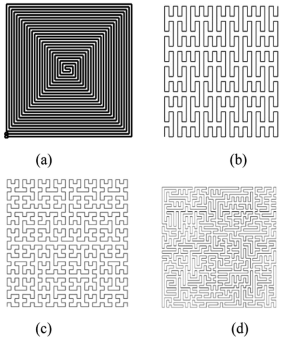
(*) This is usually the case, but some wallet makers have customized SE SW to various extents; it is difficult and not usually done.

Aside on “Countermeasure Shield“

NOTE: 28nm is naturally more resistant to attack, but effectiveness of countermeasures is also enhanced by smaller metal size.

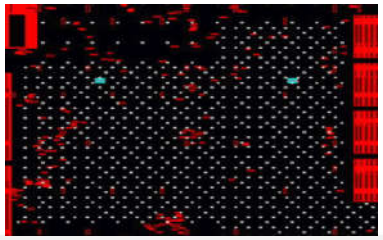
- 1. Physical Attacks (fib, probe, etc).
  - A. Active Shield
  - B. Security layout (redundant lines, dummy lines)
  - C. Security Design (self-check, dynamic logic)

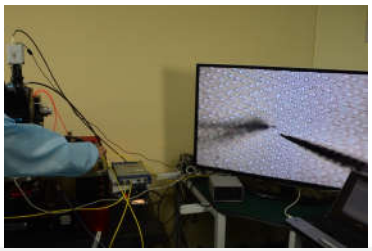
- 2. Fault Injection (laser, clock glitch, voltage glitch, EM/radiation, thermal)
- A. Glue Logic design (error coding, register mirror, write verify)
- B. Glue Cells (trigger cells) throughout chip
- C. Isolated clock
- D. Detectors (voltage, light...)



- 3. Side Channel (SPA, DPA, EM, ...)
- A. Algorithmic and implementation countermeasures
- B. Walkaround countermeasures (false operation, clock jitter, power balancing)

- 4. Other
- A. Strong/redundant lifecycle protection
- B. Multi-stage secure boot, multi-signature
- C. Memory protection (access control, encryption)
- D. Strong TRNG (multiple, self-checking)





Architectural improvements

1. Replace Flash with other memory type
   - Boot code for MCU
   - Secret storage
   - Back-up media
2. Extend Physical Countermeasure shield
   - Input, output, UI, boot, etc. functions are also attack surfaces
3. Update crypto engines to include blockchain crypto
4. Move to advanced node process (attack resistant, high performance): 28nm and beyond
5. Support user with complete devkit