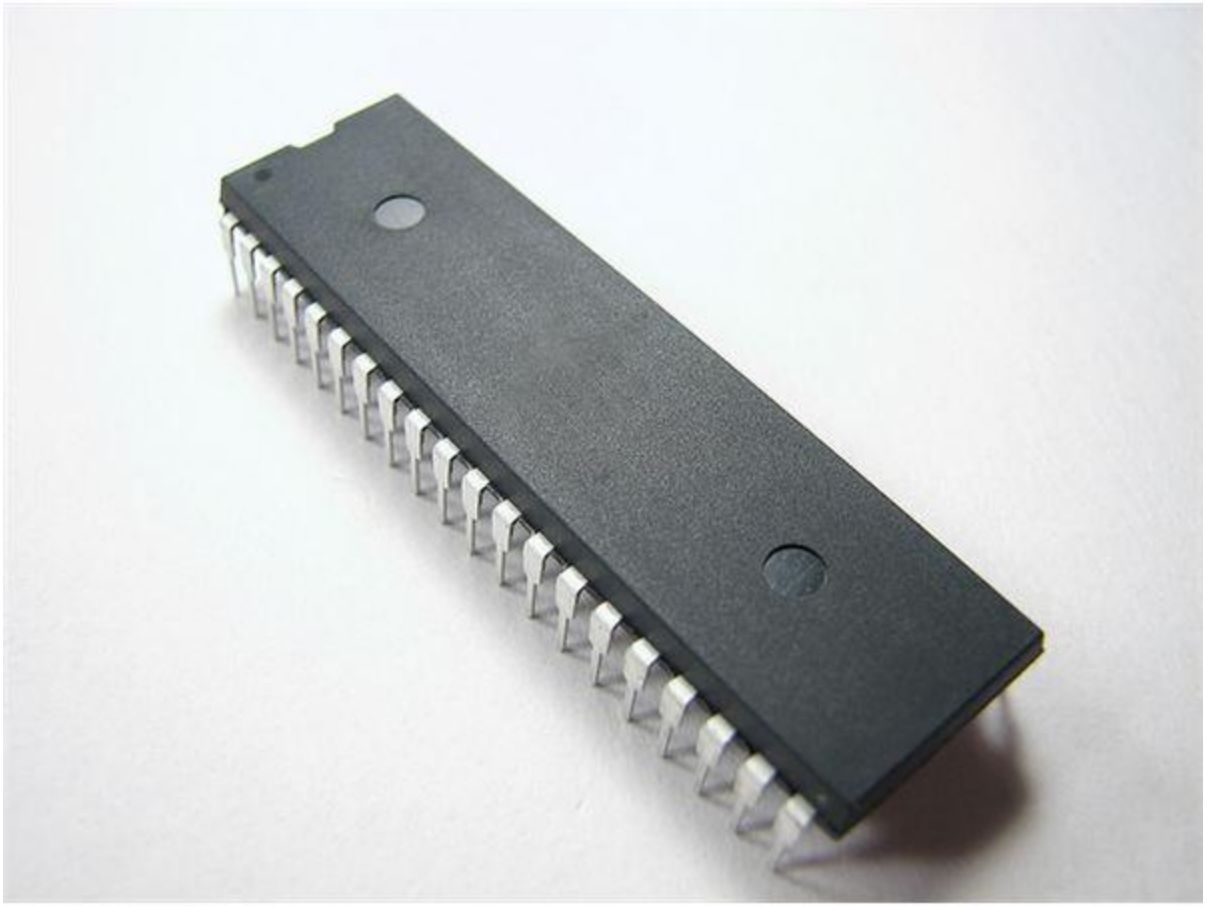
Cost effective techniques for chip delayering and in-situ depackaging

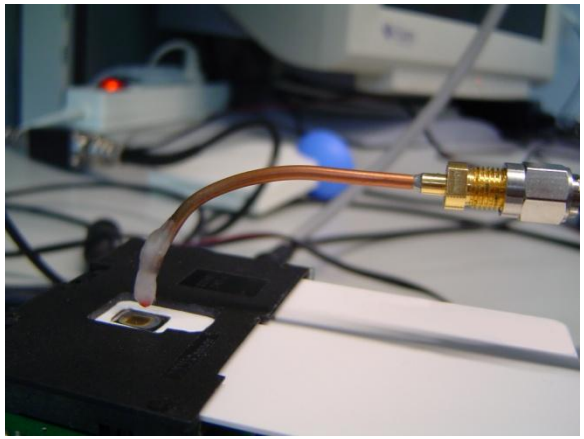
Philippe Loubet Moundi
Gemalto Security Labs

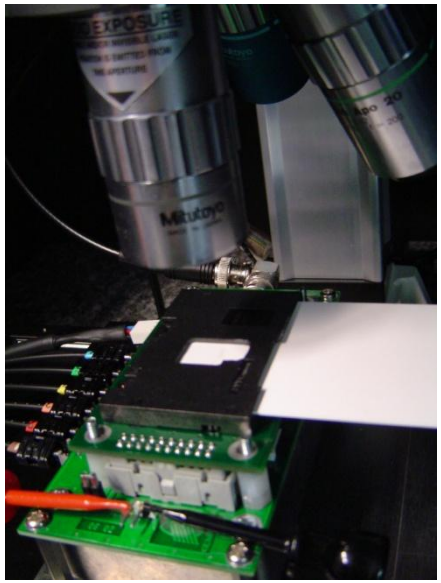
08 March 2013
COSADE 2013

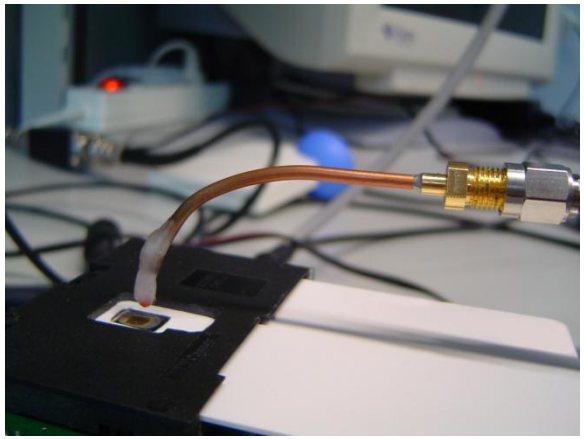
Part 1

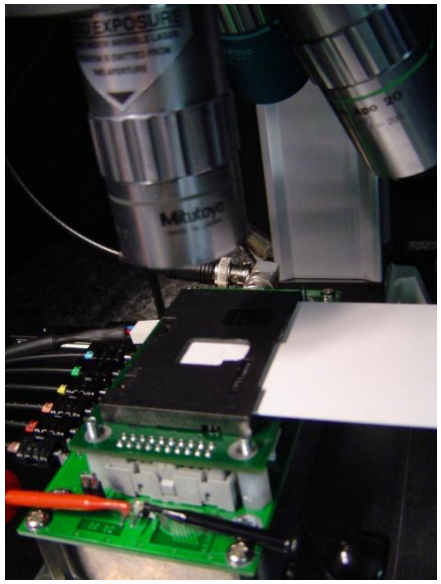
IN-SITU DECAPSULATION

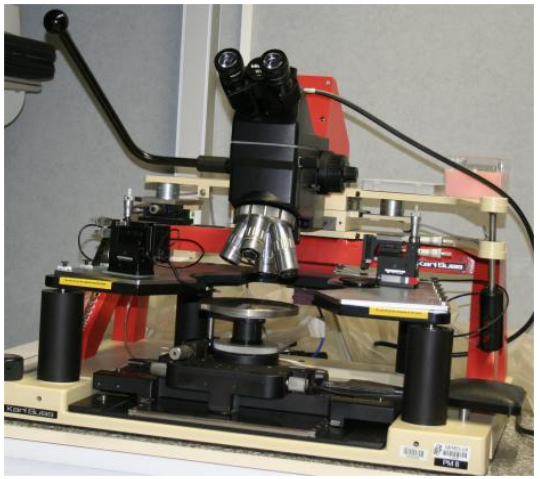


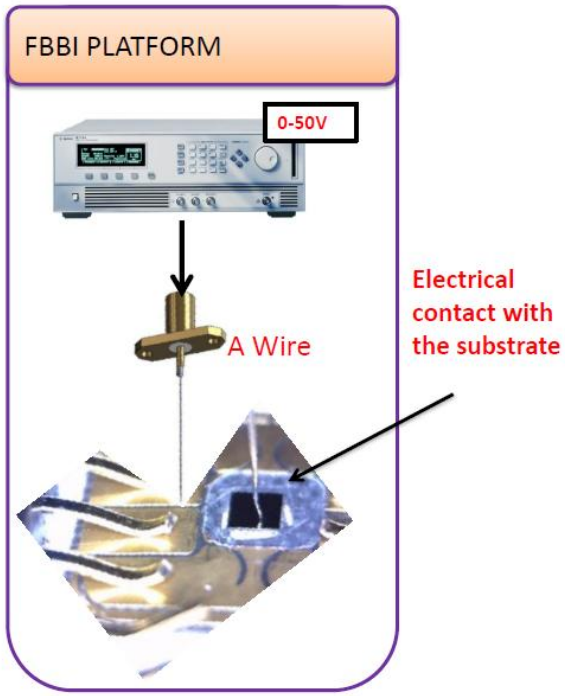



EXPOSURE
Mitutoyo









Courtesy of Ph. Maurine / LIRMM

Access to the die
Without compromising die integrity
Without compromising die bonding integrity

Access to the die Without removing the package from the system board


National
ID Card
gemalto
Bank
7897 6000 6892 5781


National
ID Card
gemalto
Bank
7897 6000 6892 5781


13542198771


National
ID Card
gemalto
Bank
7897 6000 6892 5781


13542198771


gemalto


National
ID Card
gemalto
Bank
7897 6000 6892 5781


13542198771


here


gemalto


National
ID Card
gemalto
Bank
7897 6000 6892 5781


13542198771

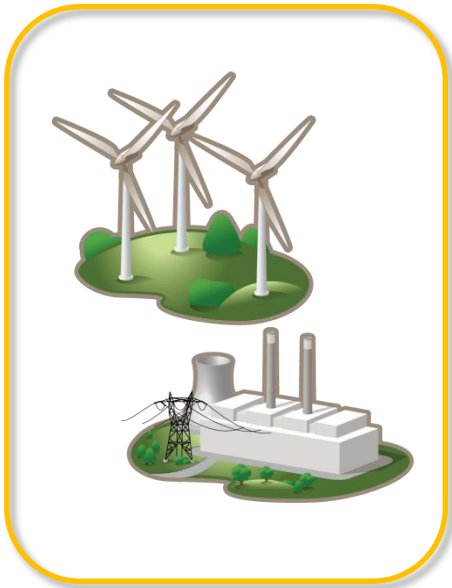

here


gemalto

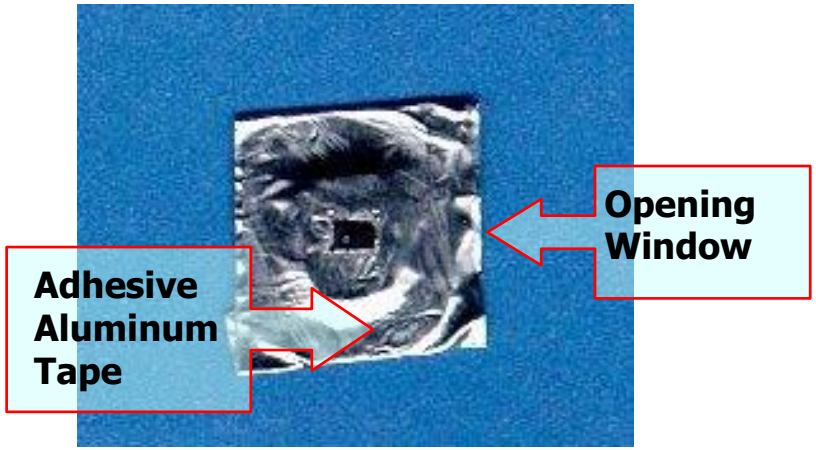

National
ID Card
gemalto
Bank
7897 6000 6892 5781

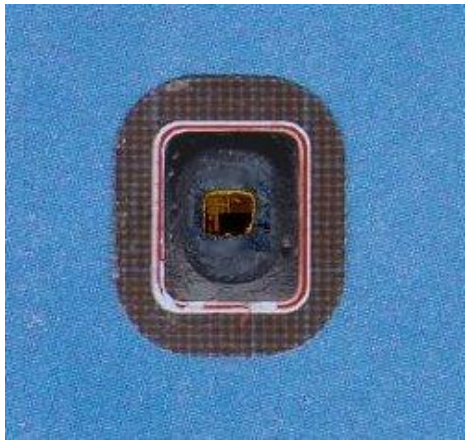

13542198771

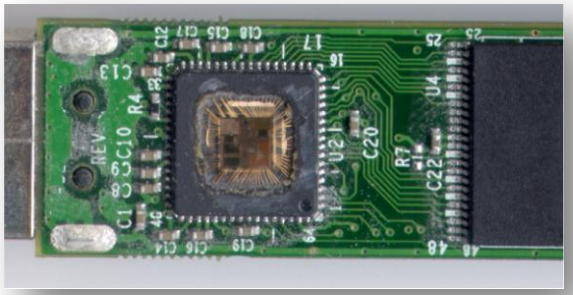

here

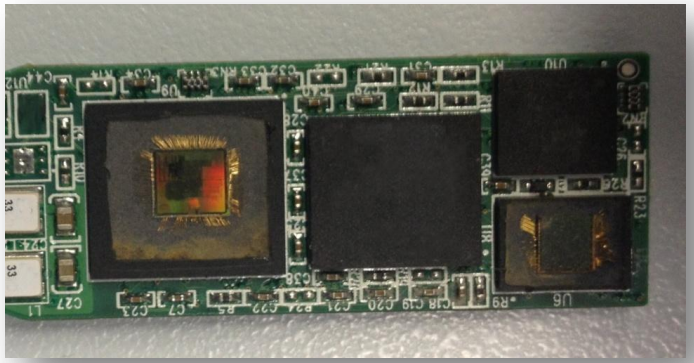


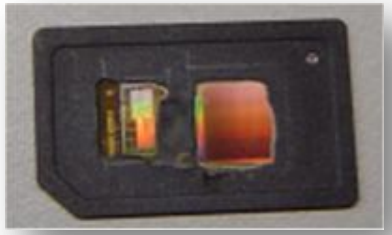

gemalto


Opening
Window
Adhesive
Aluminum
Tape













In-situ depackaging summary

Pros

- Reliability
  - Single operation
  - No damage of the PCB
- Cost
  - Tools for de-soldering/soldering ***not needed***
  - Bonding equipment ***not needed***
  - Al adhesive tape
  - Hot Fuming Nitric Acid + Water (+ Acetone) + dry air (nitrogen)

Cons

- The side of the die exposed depends of the package
  - Lucky or unlucky?
  - 3D packages

Part 2

ULTRA LOW COST DELAYERING

Ultra low cost sample preparation

200K€

Ultra low cost sample preparation

Ultra low cost sample preparation

50K€

Ultra low cost sample preparation

50K€

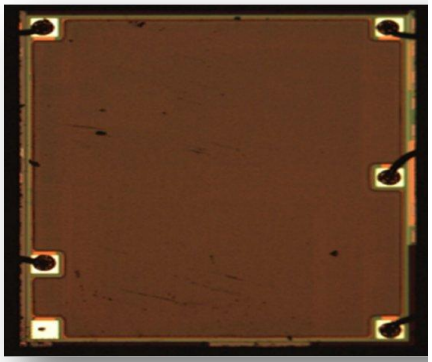
Ultra low cost sample preparation

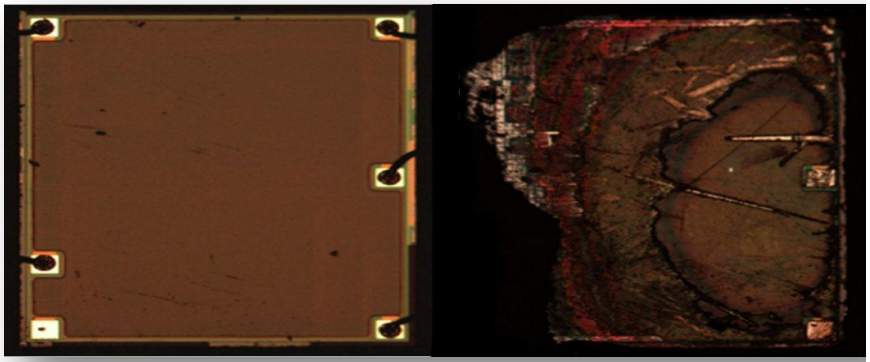
50K€

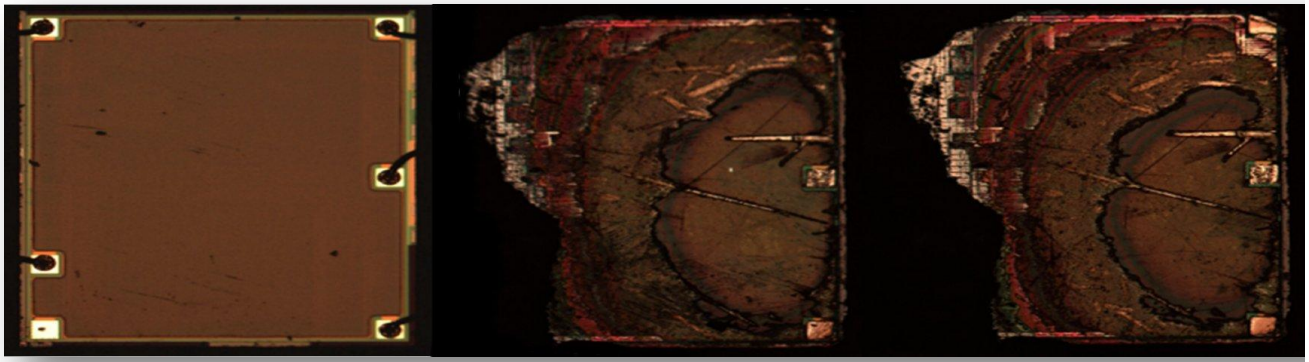
Ultra low cost sample preparation

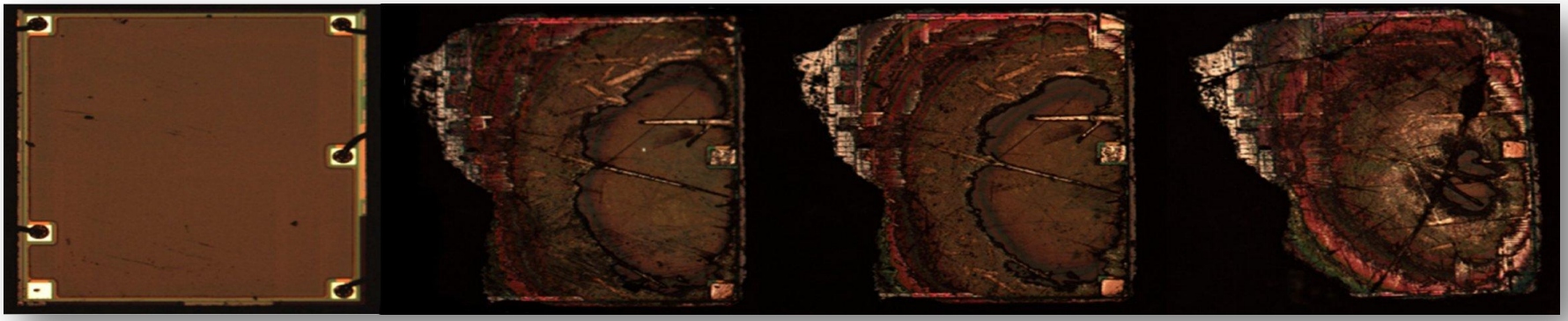
50K€

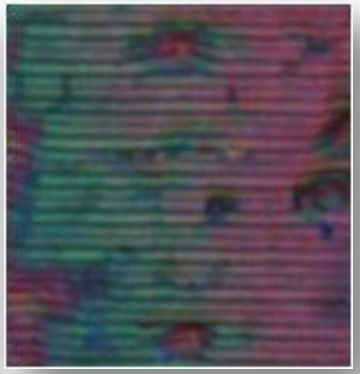
Ultra low cost sample preparation

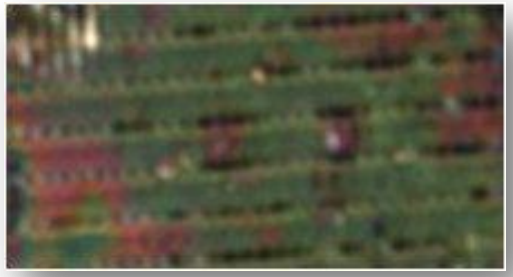


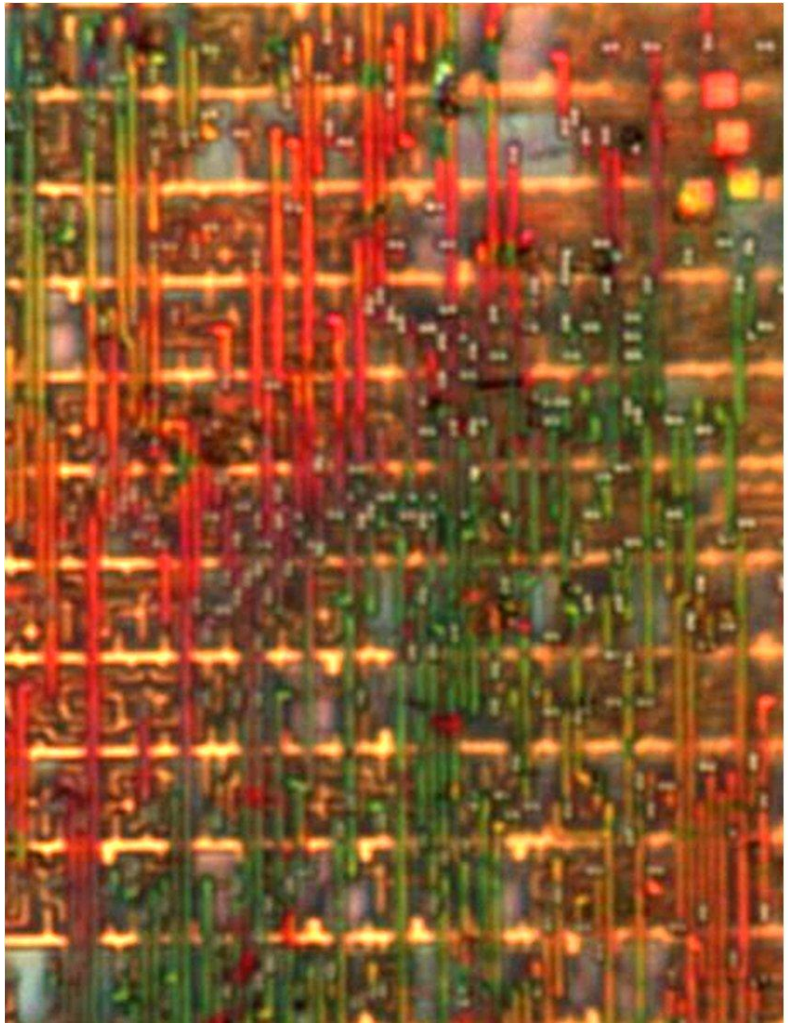


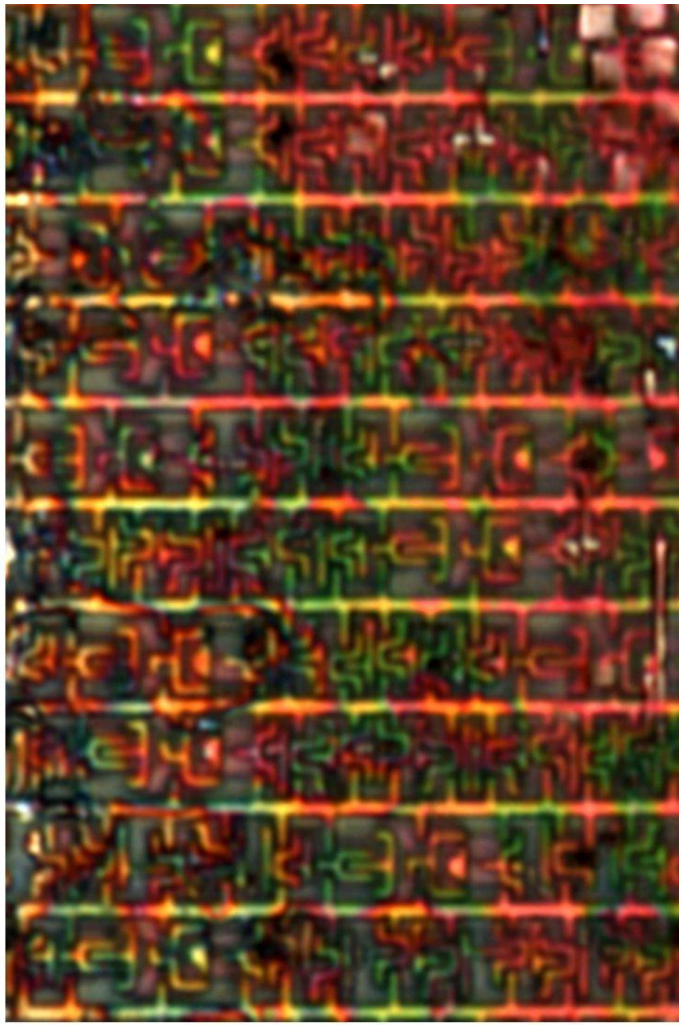


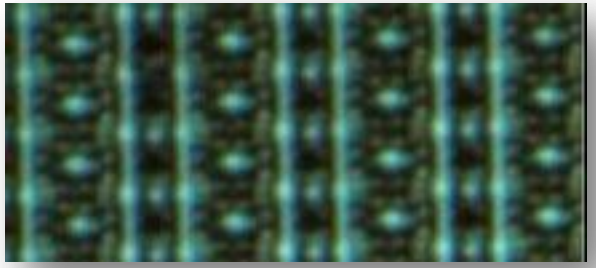


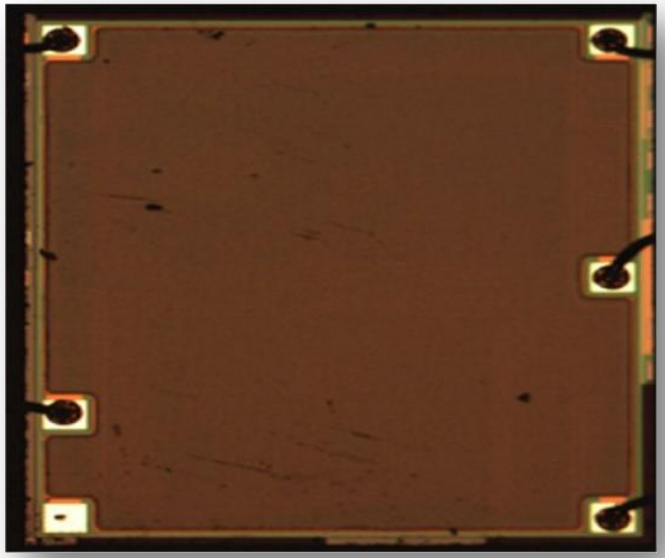



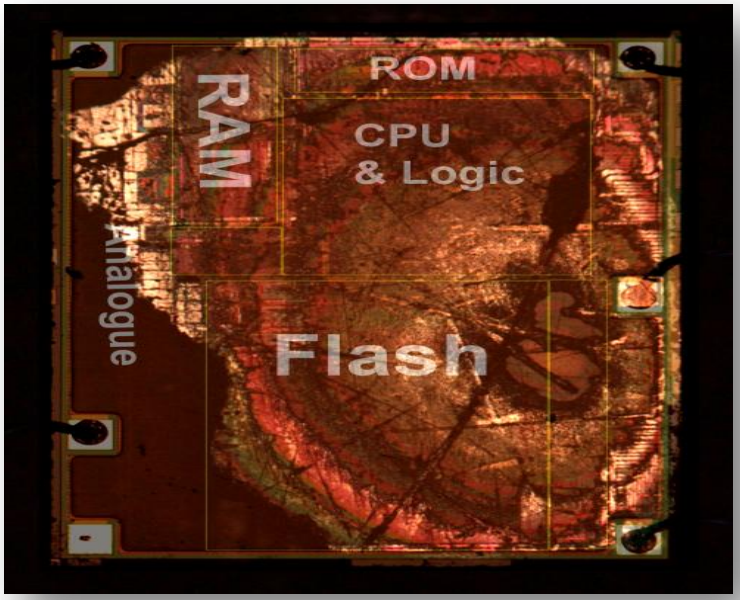











ROM
RAM
CPU
& Logic
Analogue
Flash

Ultra Low Cost Delayering (DJ, Die Jittering) Summary

- Of course, DJ sample preparation technique can be seen as a proof of concept
- But…
- It shows that very expensive equipments are not mandatory to get chip hidden data

CONCLUSION

Conclusion

- Cost effective techniques could (must?) be used for improving attacks
- Low cost in-situ depackaging gives significant advantages compare to chip extraction
- Ultra low cost sample preparation could gives very interesting information

- Having inside knowledge of the attacked chip is often the first step of a successful physical attack

Conclusion

- Cost effective techniques could (must?) be used for improving attacks
- Low cost in-situ depackaging gives significant advantages compare to chip extraction
- Ultra low cost sample preparation could gives very interesting information

- Having inside knowledge of the attacked chip is often the first step of a successful physical attack

So, try it !


They are ready to try
THANK YOU FOR YOUR ATTENTION