THALES

INVIA
IPs securing ICs

Why should your next secure design be PUF based?

Christophe TREMLET, Marketing & Sales Director
Vincent TELANDRO, Sales Manager

Design & Re-Use Bay Virtual Event Apr 20

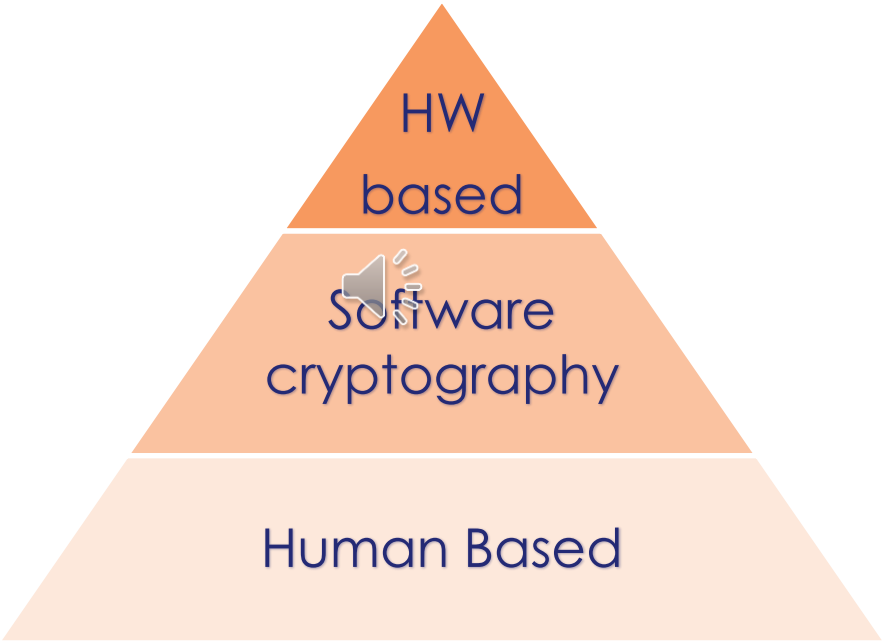
Why Should Your Next Design be PUF Based: Outline

INVIA

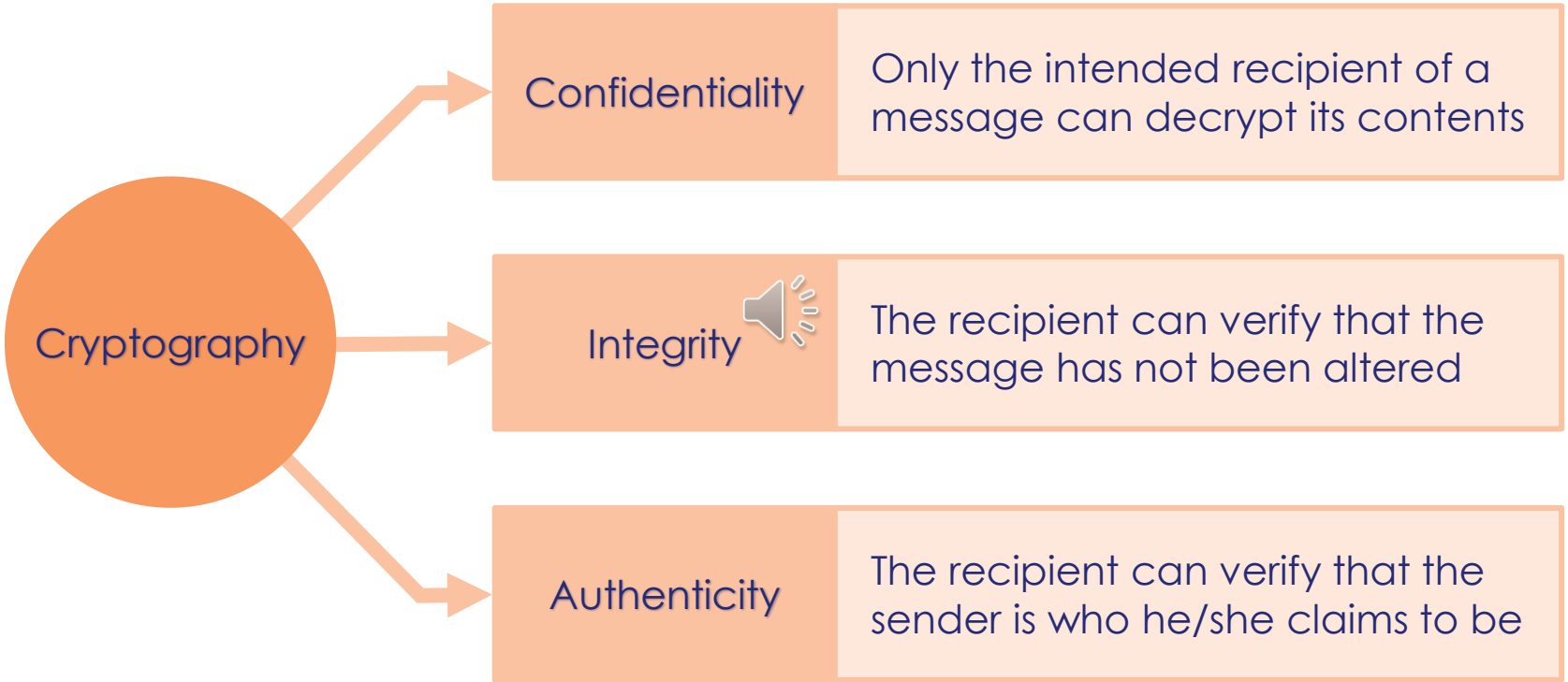
- Introduction to Embedded Security And Cryptography
- Keys Protection Challenge
- PUF Fundamentals
- INVIA's PUF Solution And Its Benefits

Hierarchy in Security Measures

INVIA



Cryptography Supports The 3 Security Pillars

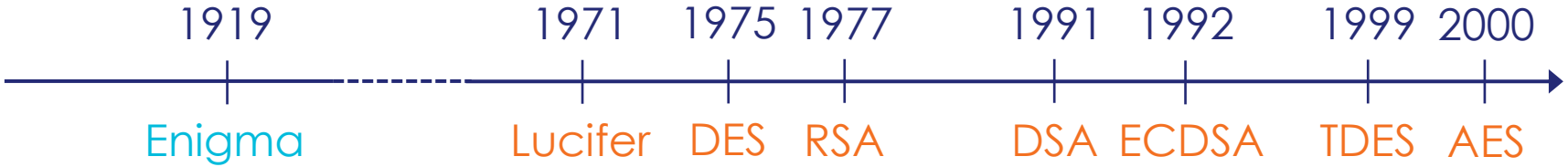


Modern Cryptography

INVIA

Secret algorithm

Public algorithm / Secret key



Secret Key – Attacks

INVIA

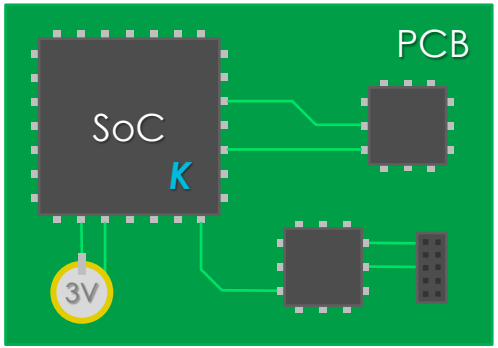
Non-invasive attacks

Passive (observation)

- On-board probing
- Side-channel attacks

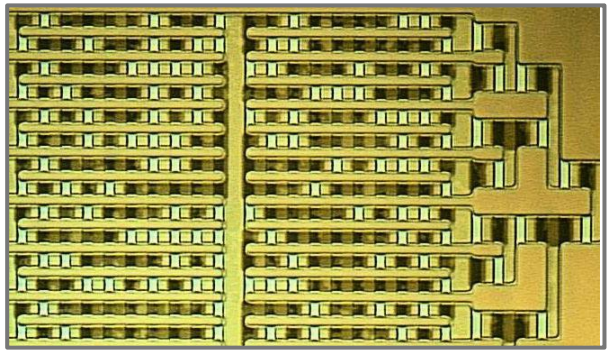
Active (perturbation)

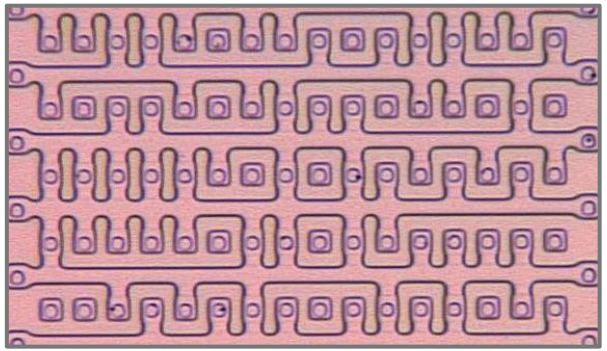
- Over/under V, T° or clock
- Voltage, laser, clock or EM glitchs



Invasive attacks

- Chemical & laser etching
- On-chip microprobing
- Layout reconstruction
- Memory content recovery
- Electron Beam Tester (EBT)
- FIB-SEM nanofabrication



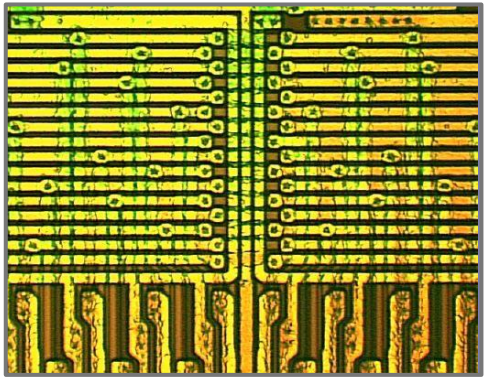


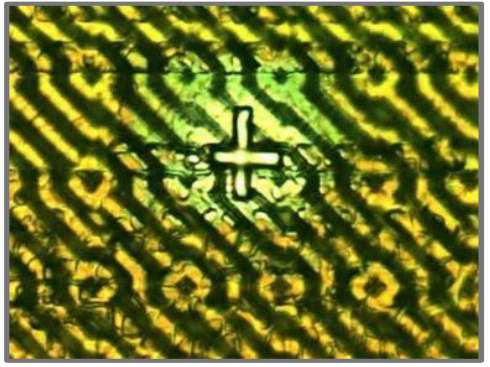
Secret Keys Protection

INVIA

Protect keys

- **Sensors**
  - Voltage
  - Temperature
  - Clock
  - Laser & EM pulses
- **Cryptography**
  - Key diversification
  - Memory encryption
- **Obfuscation**
  - Bus scrambling
  - Random P&R
  - Shield: metal mesh
  - Power randomisation





OPEN

Physical Unclonable Function (PUF)

INVIA

Principle	➢ Acts as a device fingerprint ➢ Generates a per-chip unique identifier ➢ Exploits the random variations of the devices' parameters
Benefits	➢ Much stronger protection than obfuscation ➢ Key generation without storage ➢ Accessible without security knowledge as an IP block ➢ Ground for full security of an ASIC / SoC

Physical Unclonable Function (PUF)

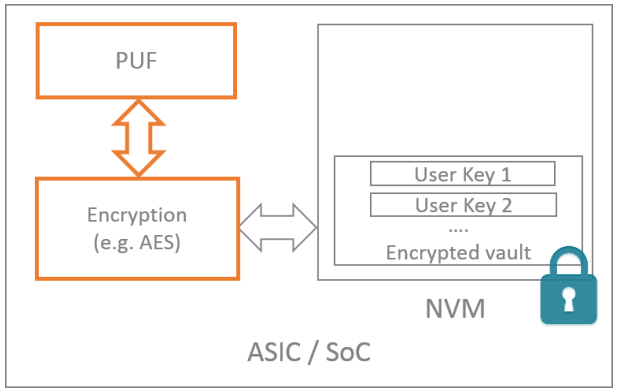
INVIA

Challenges	
	➢ Unclonable: robust against counterfeiting ➢ Uncontrollable: robust against invasive attacks ➢ Unpredictable: robust against reverse engineering ➢ Invariant: stable across voltage, temperature and aging

PUF Use Cases

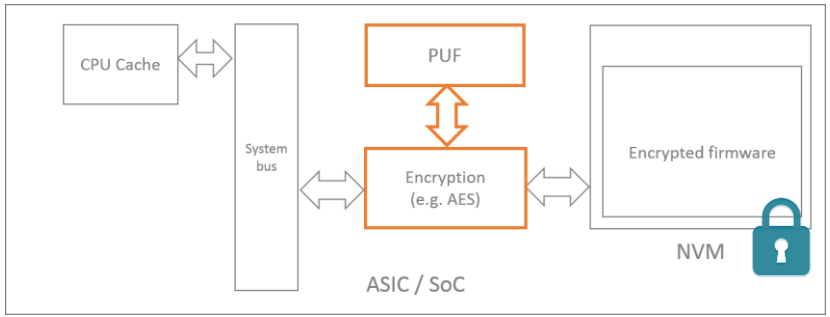
INVIA

Key Vault



- Keys are the most valuable assets
- Physical key protection available to non security experts
- Stronger than obfuscation

Software IP Protection

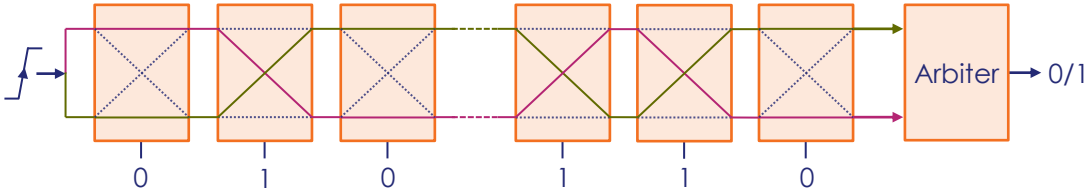


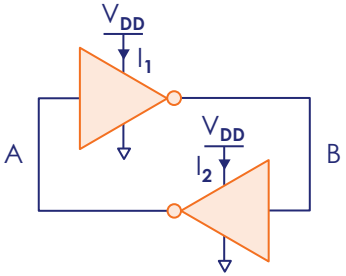
- Software IP is gaining value
- PUF with encryption
  - provides the strongest protection
  - enables revenue protection

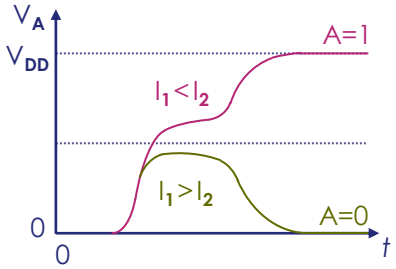
PUF – Examples

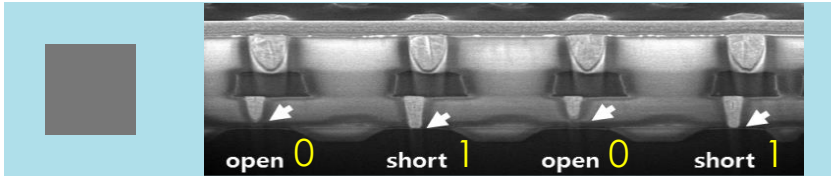
INVIA

Delay based	➢ Arbiter ➢ Ring oscillator ➢ Glitch
Memory based	➢ SRAM ➢ Latch
Process based	➢ V_{GS} or V_{DS} ➢ Via



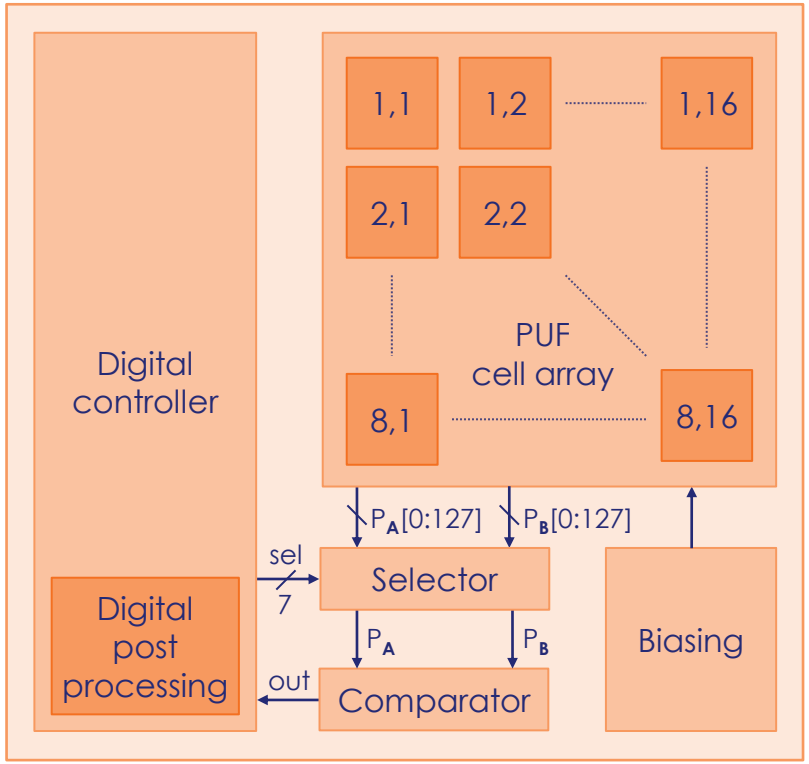


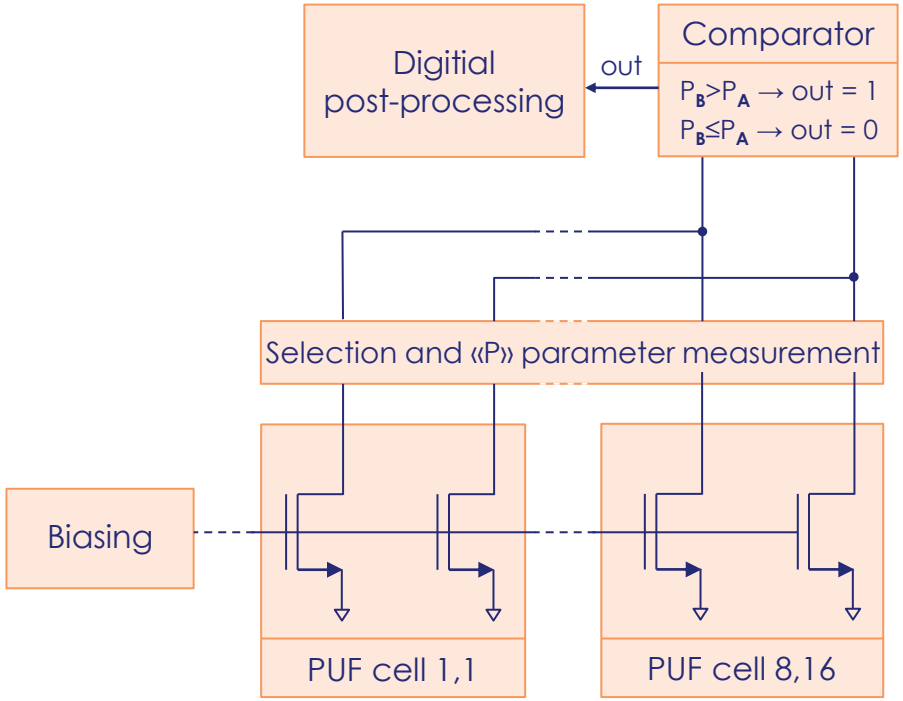




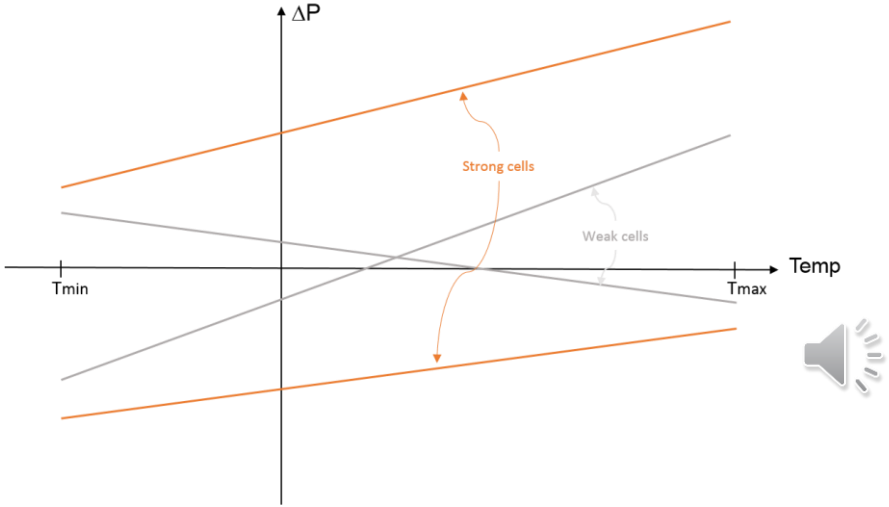
OPEN

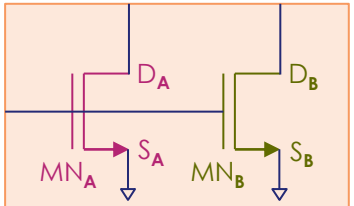
Invia's PUF – Principle (patented)



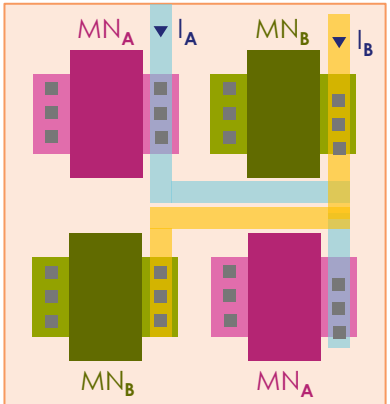


Invia's PUF – Reliabiluty





PUF cell - Schematic



PUF cell - Layout

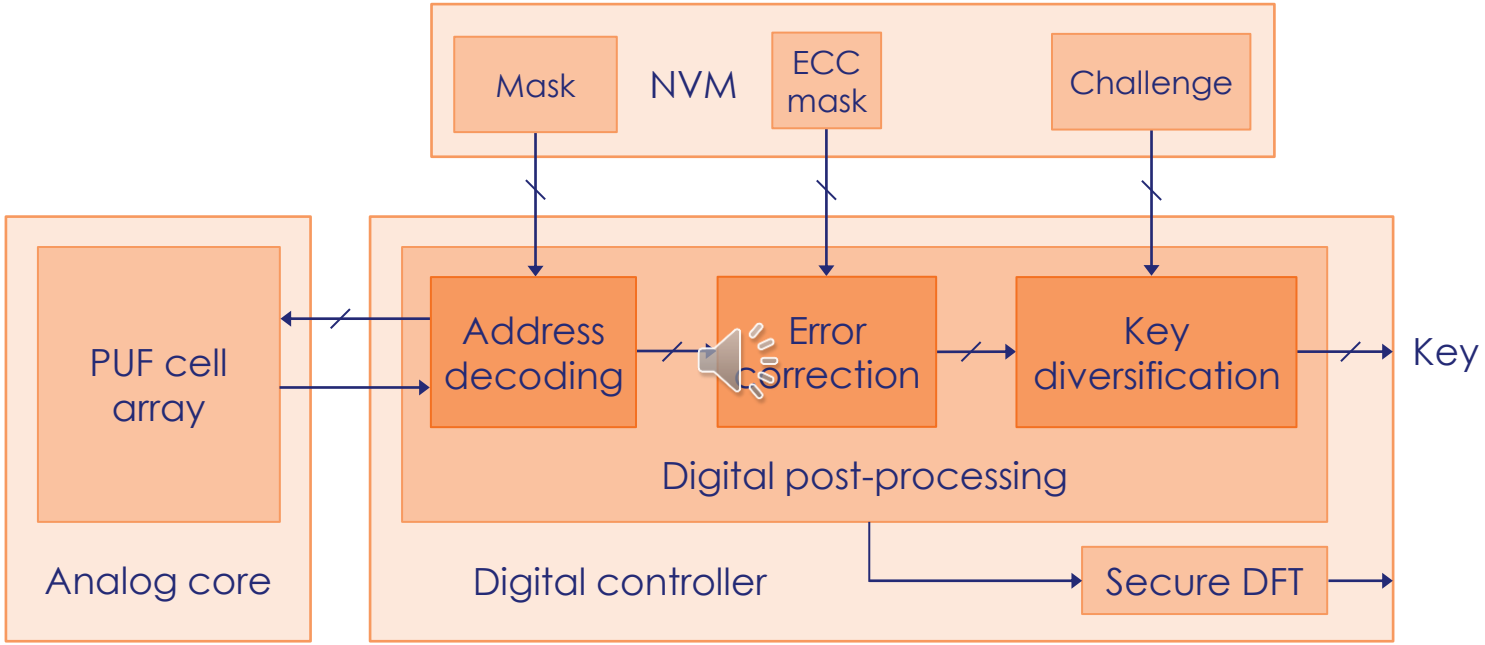
Weak cells are discarded

Naturally reliable

- 100 million PUF deployed
- 1.7 B bits tested
- 5 ppm before error correction

Invia's PUF – Digital post-processing

INVIA



Enables multiple keys generation to support « one key for one usage »

Invia's PUF – Facts And Benefits

INVIA

Performances (f_{clk}=50 MHz)	➢ Active current < 10 µA ➢ Stby current < 10 nA ➢ First key < 210 µs ➢ Next keys < 20 µs

Size	➢ Digital < 15 kgates ➢ Analog < 0.02 mm²

Benefits	➢ **Low-power**: consumption significantly smaller than most aternatives ➢ **Modelled**: means robust and certifiable ➢ **Stable and reliable**: sigma optimized by design ➢ **Secure**: active monitoring of the sub-blocks' integrity ➢ **Scalable**: the smaller the node, the better the gaussian distribution

Takeaways

INVIA

INVIA, a Thales company

- Conducts exhaustive security audits
- Assists companies in securing their systems
- Delivers silicon-proven IPs part of EAL5+ ASICs
- Protects more than 2.0 billion deployed devices

Thank you for your attention