Can we build a Trustworthy Billion Transistor Chip?

Samuel Pagliarini

Senior Research Scientist

Carnegie Mellon University

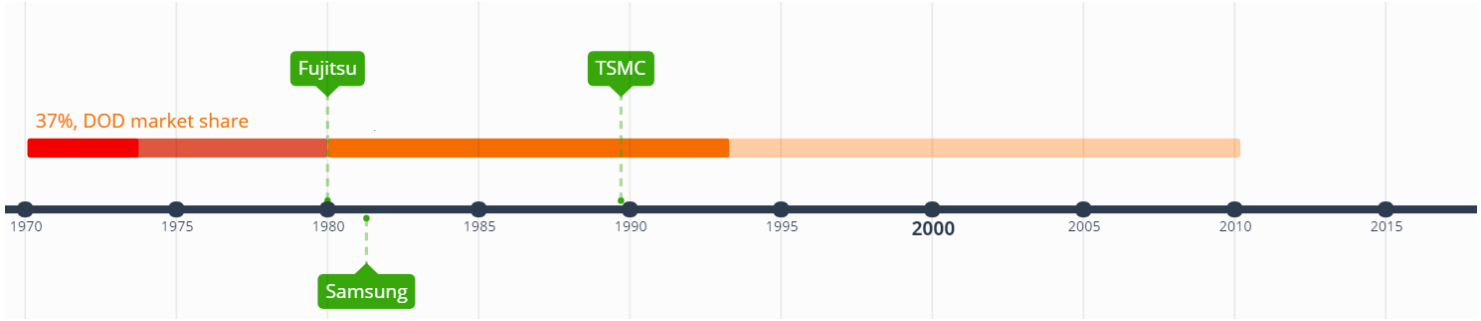
Electrical & Computer ENGINEERING

Acknowledgment

Can we build a **Trust**worthy Billion Transistor Chip?

The DoD saga in microelectronics

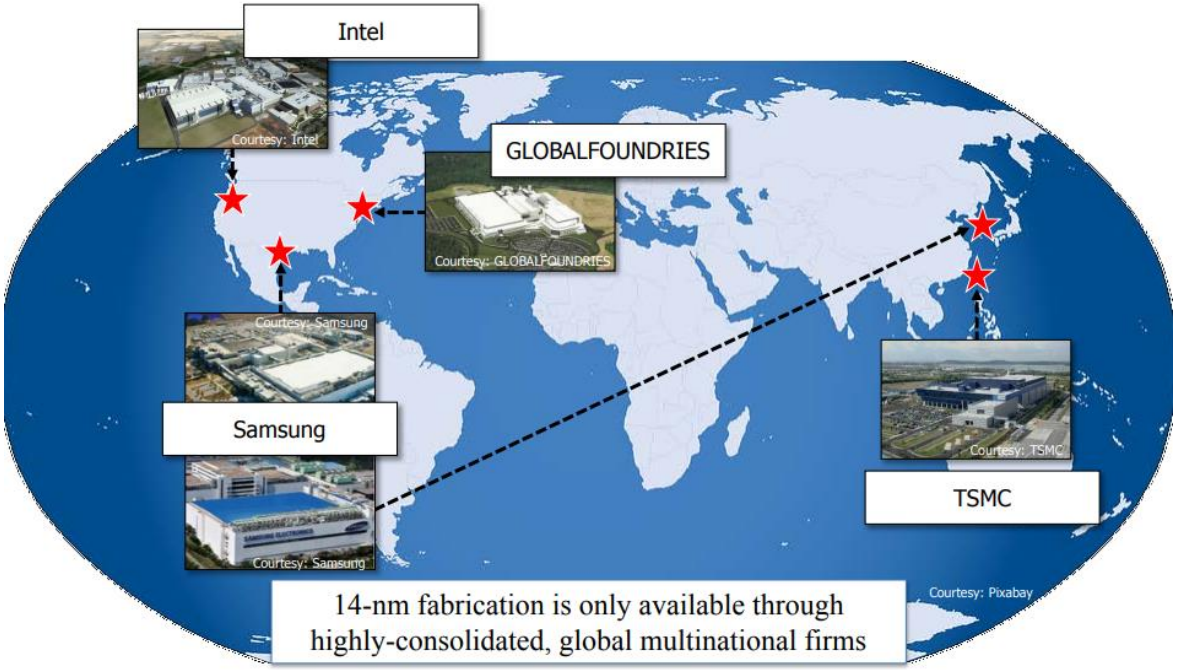
- **Semiconductor** industry began in the United States
- The US government procured **37% of all the ICs** (1970)
  - Space and defence were the big drivers of the innovation
- Japan and Korea took over the memory market (Fujitsu and Samsung, 1980)
- Taiwan enters the scene with the first **fab-for-hire** (TSMC, 1990)
- Early 2000s, reports already point out that the US will **lose access** to cutting edge silicon



The DoD saga in microelectronics

1970: Foundries were plenty, everyone had their own foundry

Today: Only one **trusted foundry** in the US, obsolete and expensive to maintain



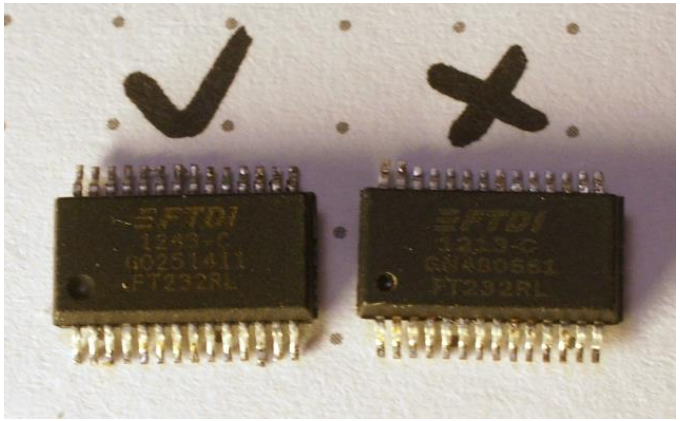
A technology-enabled new trust approach, DARPA MTO

EXCELLENT RESEARCH OPPORTUNITY!

Hardware Security

- Different meanings to different folks

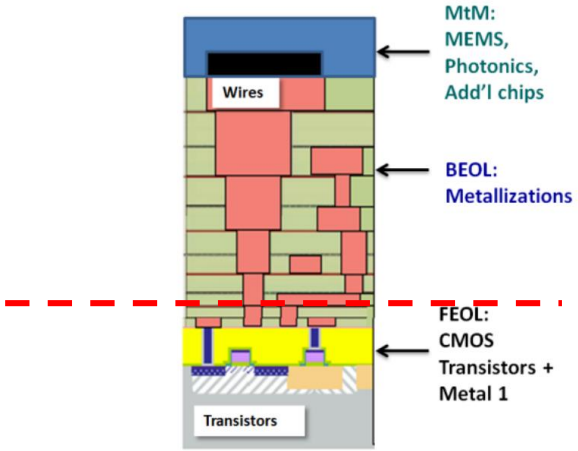
- Threat-based view of the problem
  - Counterfeit chips
  - IP piracy / IC overbuilding
  - **Reverse engineering**
  - **Hardware Trojans**
  - Side channel attacks

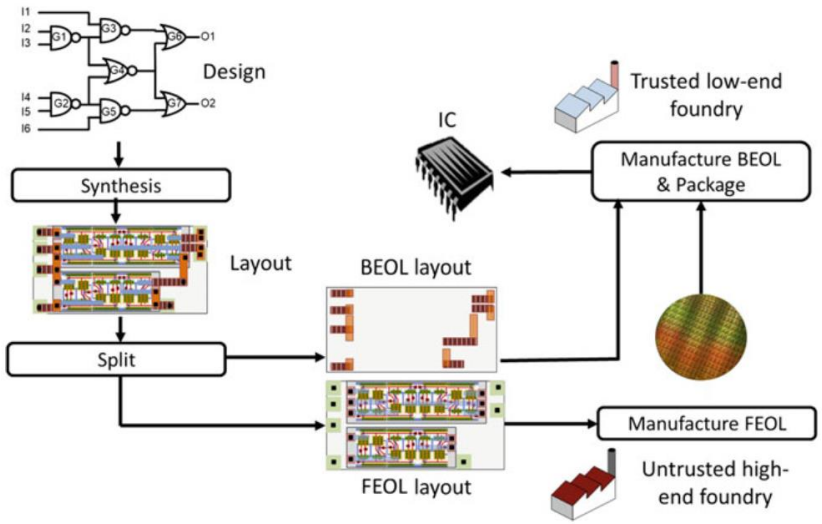


USB-to-UART chip from FTDI

CMU: Pioneers in Split-Fabrication

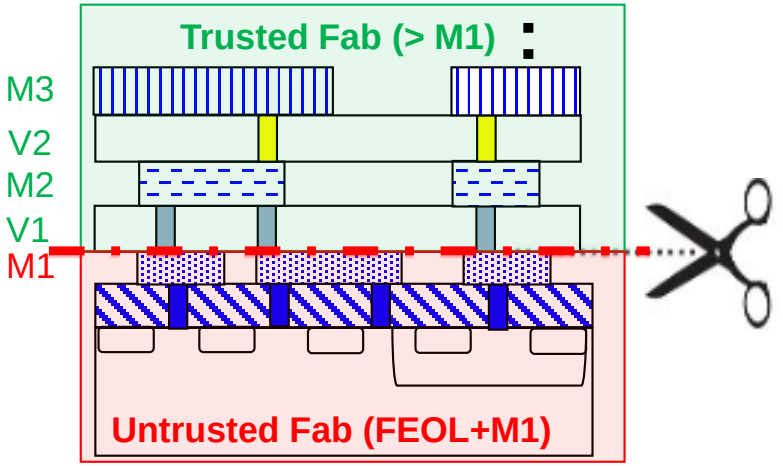
- **Hybrid manufacturing solution**
  - Trusted fab
  - Untrusted fab
- Leverages the **high-performance** of untrusted fabrication (fast and power efficient transistors)
- Mitigates **trojan insertion**
- Prevents **IP theft**
- Successfully demonstrated on different foundries/techs





Drawbacks of Split-Fabrication

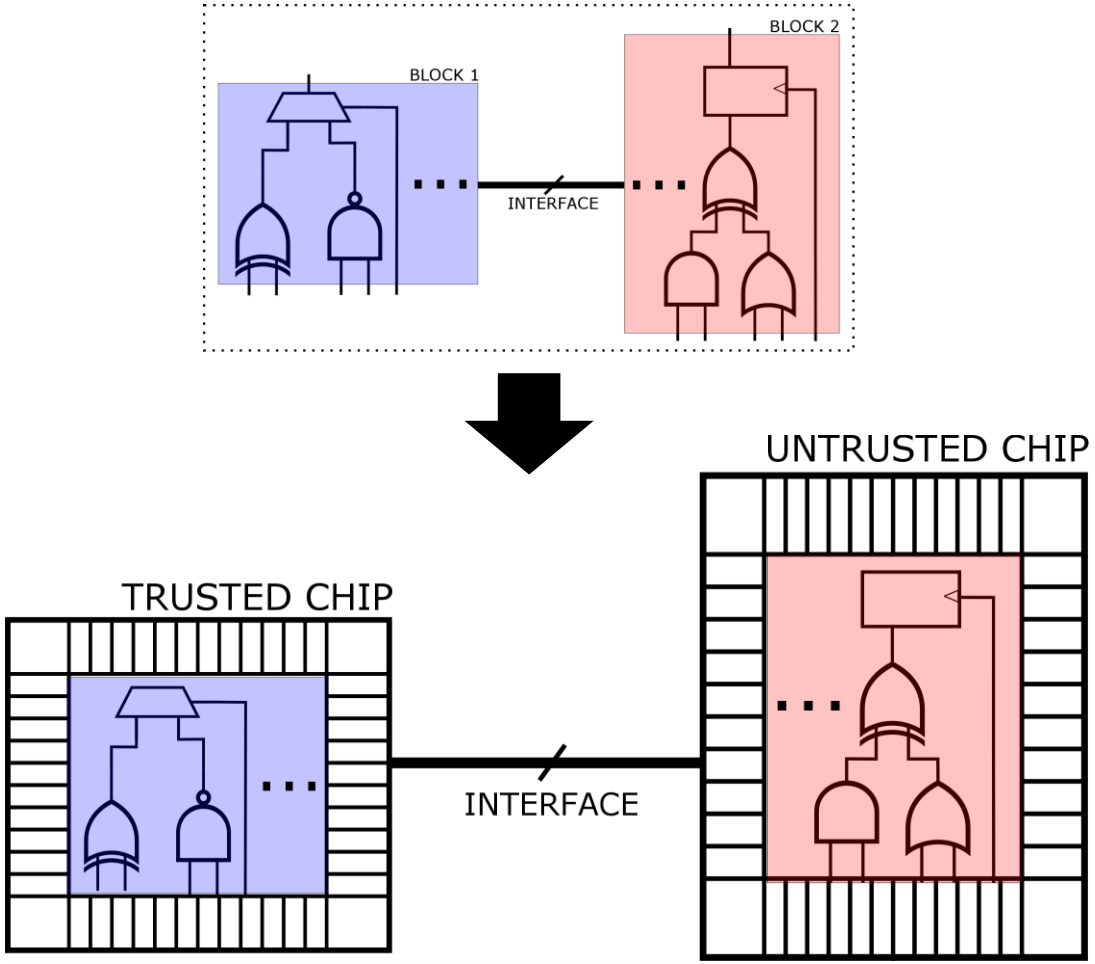
- Hybrid PDK needed
- Yield assignment?
- Alignment concerns?
- Finding foundries willing to play along ☹



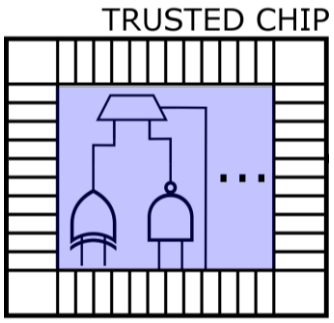
ALTERNATIVE TO HIDE DESIGN INTENT FROM FOUNDRY?

Split-Chip Methodology

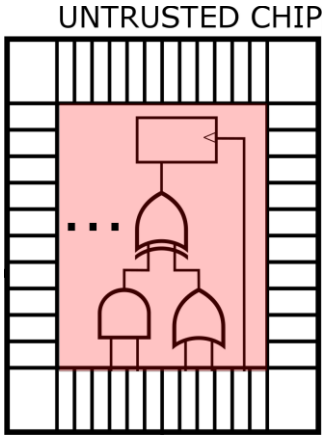
- Core concept: one design, two chips
- May have ‘zero’ performance loss if split thoughtfully



Split-Chip Methodology for ASICs



- Domestic & trusted foundry
- Legacy technology node
- Control oriented

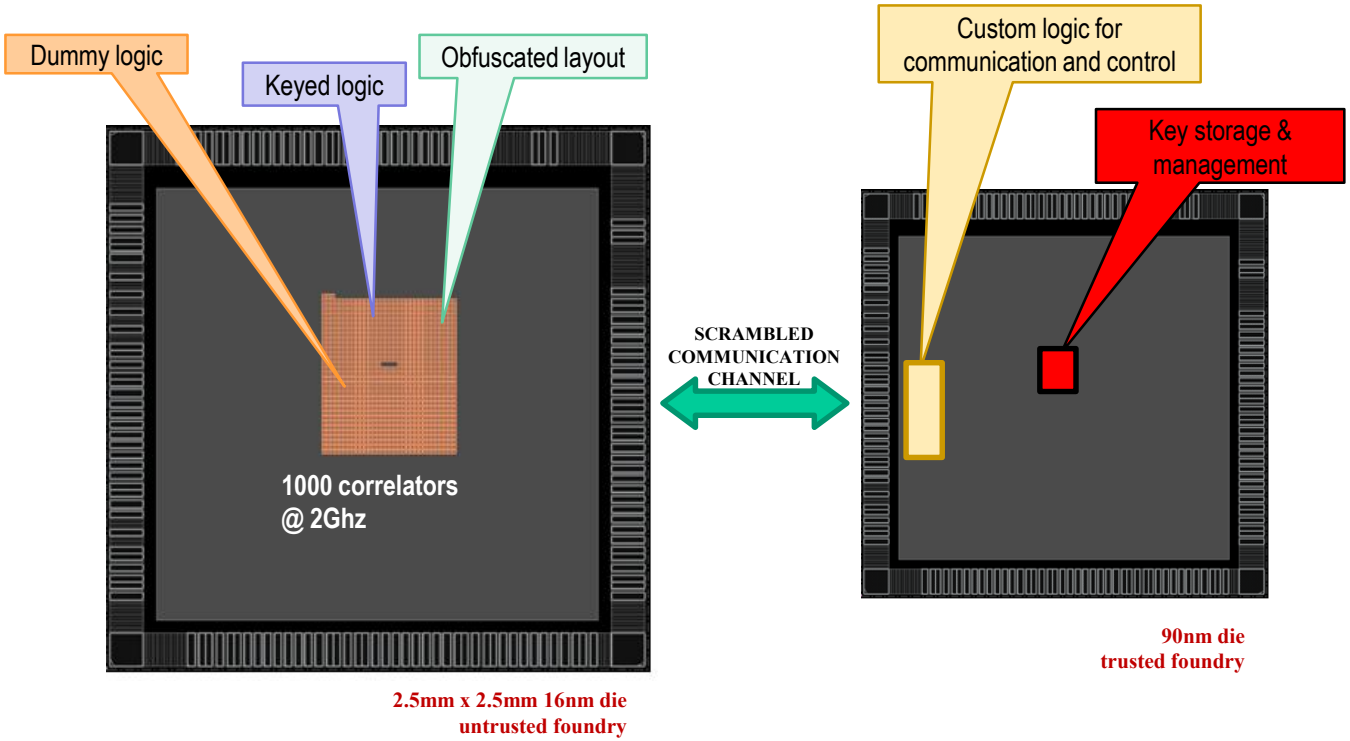


- Offshore & untrusted foundry
- High performance, high density
- Data oriented, efficient processing

- Three demonstration vehicles in 16nm FinFET

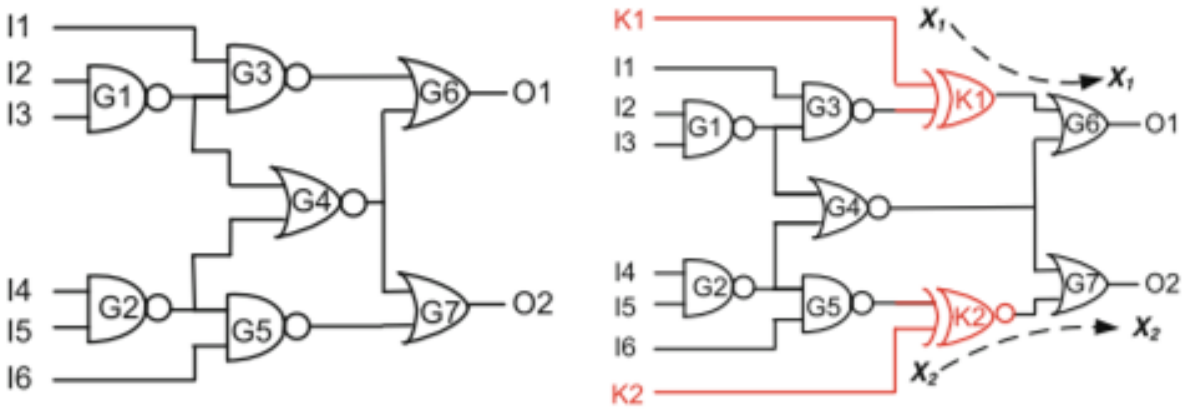
Silicon Demonstration #1

- 1000 GPS correlators @ 2GHz
- Master/slave architecture
- Additional hardware security techniques
  - **Dummy logic**, keyed logic, layout obfuscation



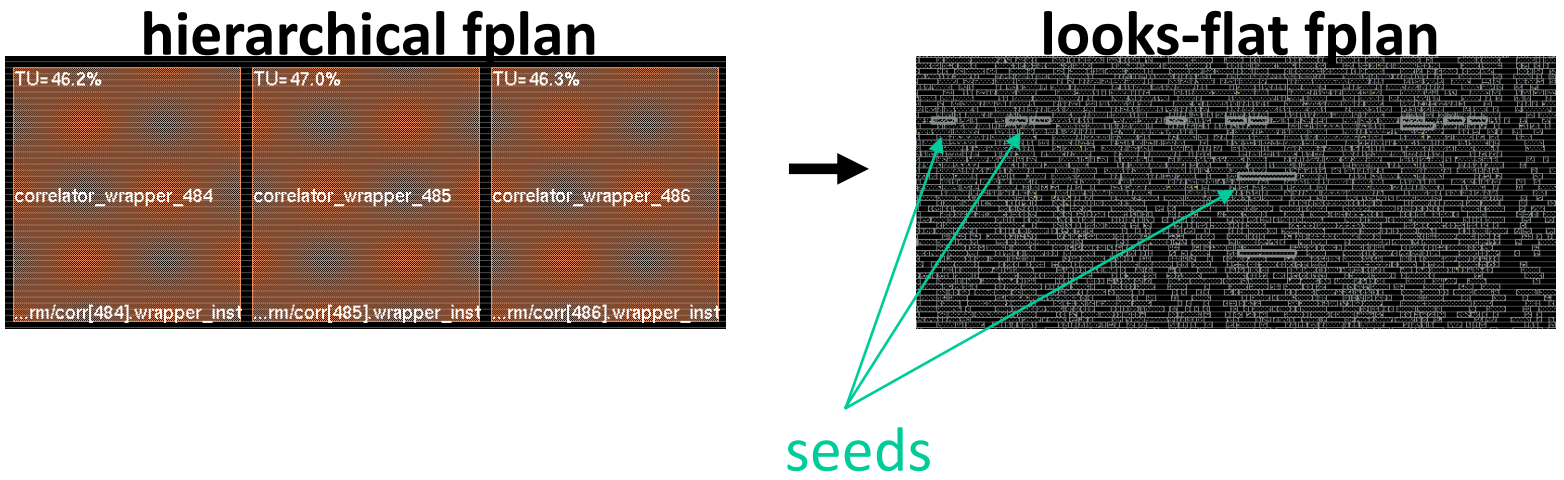
Keyed logic

- Insertion of XOR/XNOR gates and key inputs
- Circuit output is corrupted if incorrect key is applied
- Effective against **IP theft**
  - Relies on a (post) programmed memory



Lightweight Layout Obfuscation

- Grouping cells into blocks makes physical synthesis tractable, but clustering cells possibly exposes intent

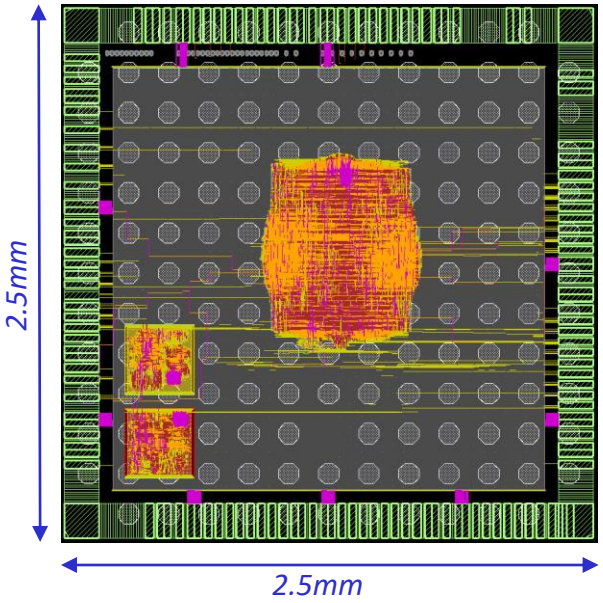


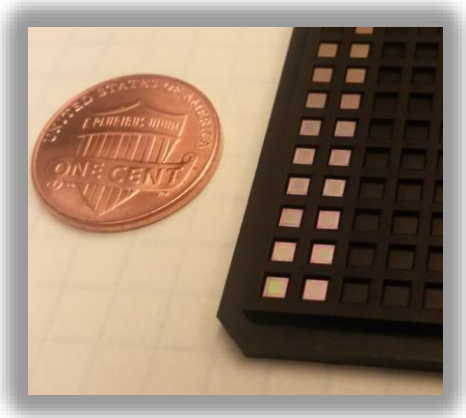
- Seeding can guarantee each correlator has a unique layout
  - The aggregate of scrambled correlators looks like random logic
  - Automated approach to achieve lightweight obfuscation

Silicon Demonstration #1

- **Manual decisions**
  - Where to split the hierarchy
  - Communication between chips (encryption?)

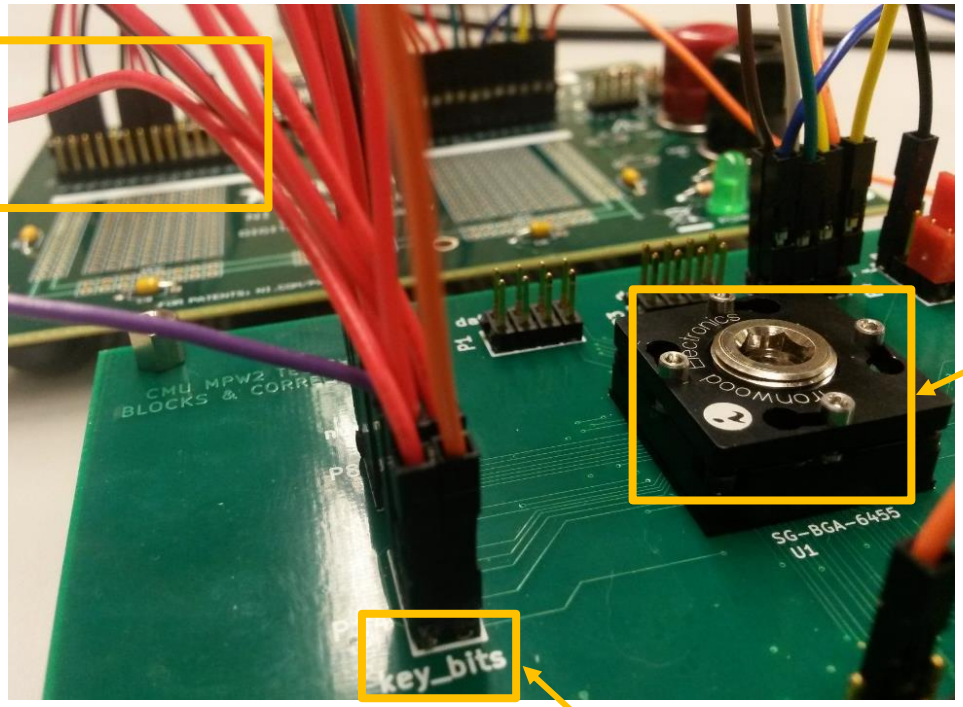
- **Lessons learned**
  - Complex trade-offs: bandwidth & latency vs security
  - Very design specific. Automation possible?





Silicon Validation

- Split-Chip GPS correlators verified to be functional
  - Zero performance loss



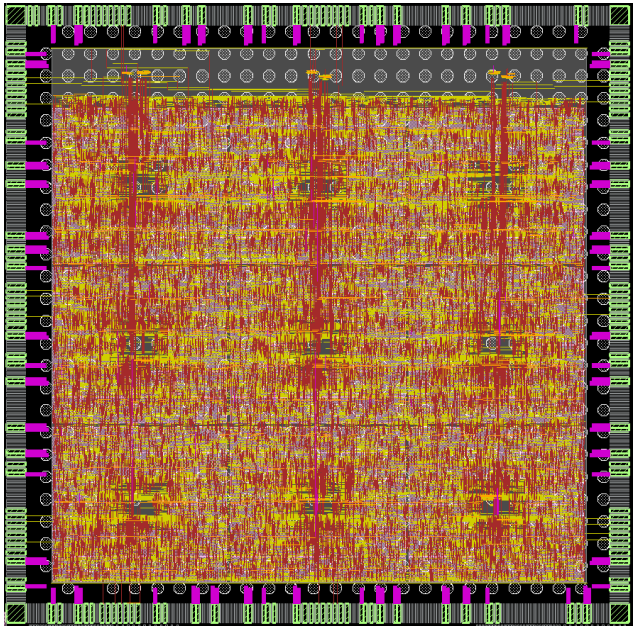
test equipment, acts as trusted IC

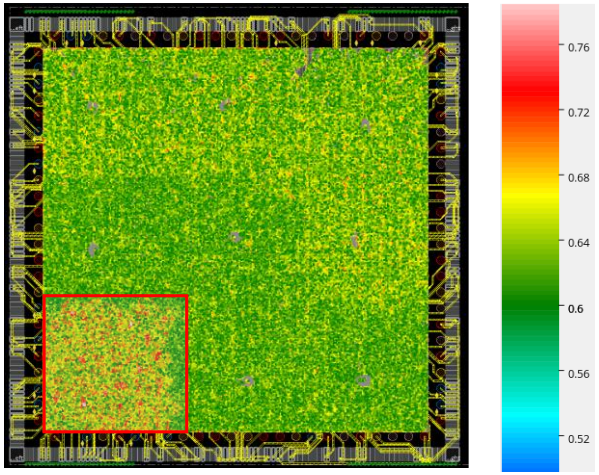
Correlator chip, acts as untrusted IC

key bits from trusted

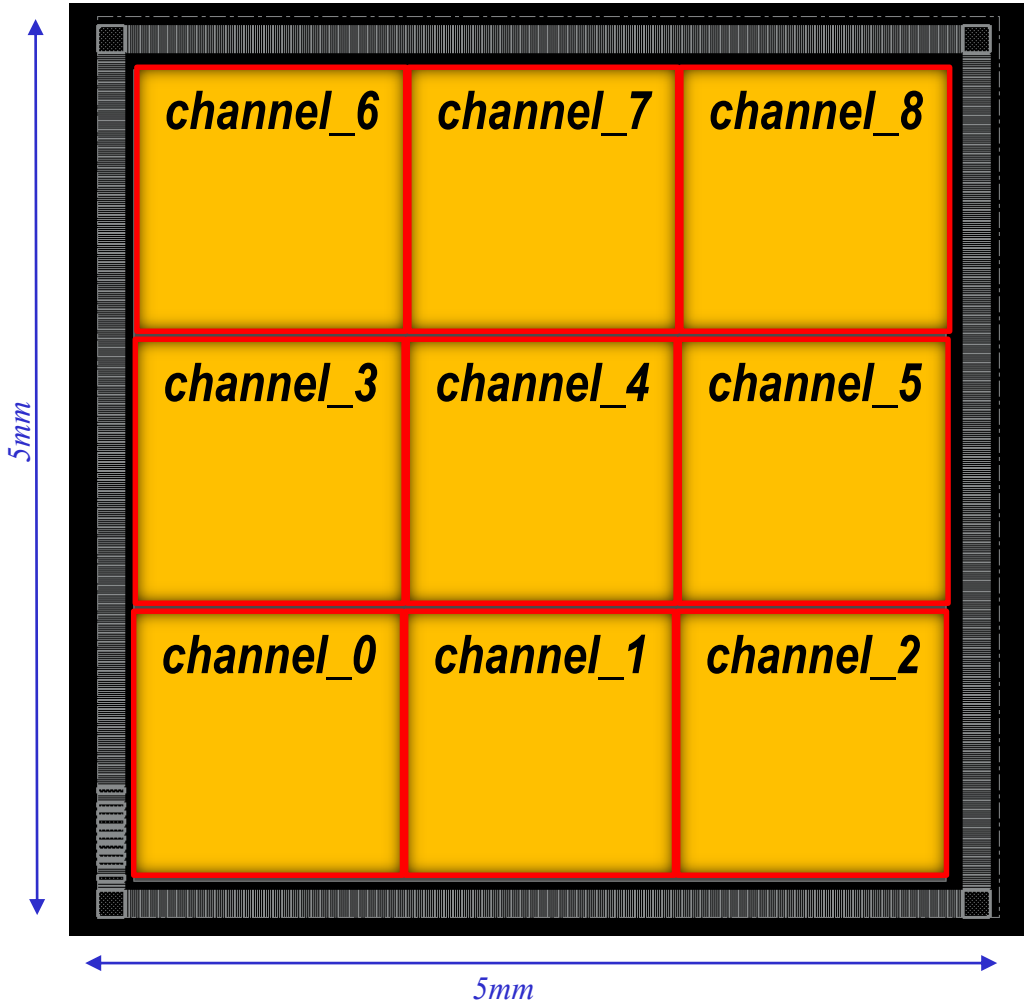
Silicon Demonstration #2

- Design characteristics
  - 300k correlators in a 5mm x 5mm die
  - Corresponds to approximately 20M standard cells (high density)
  - 5 clock domains (2.4GHz to 1MHz)
  - Floorplan organized in a 3x3 matrix





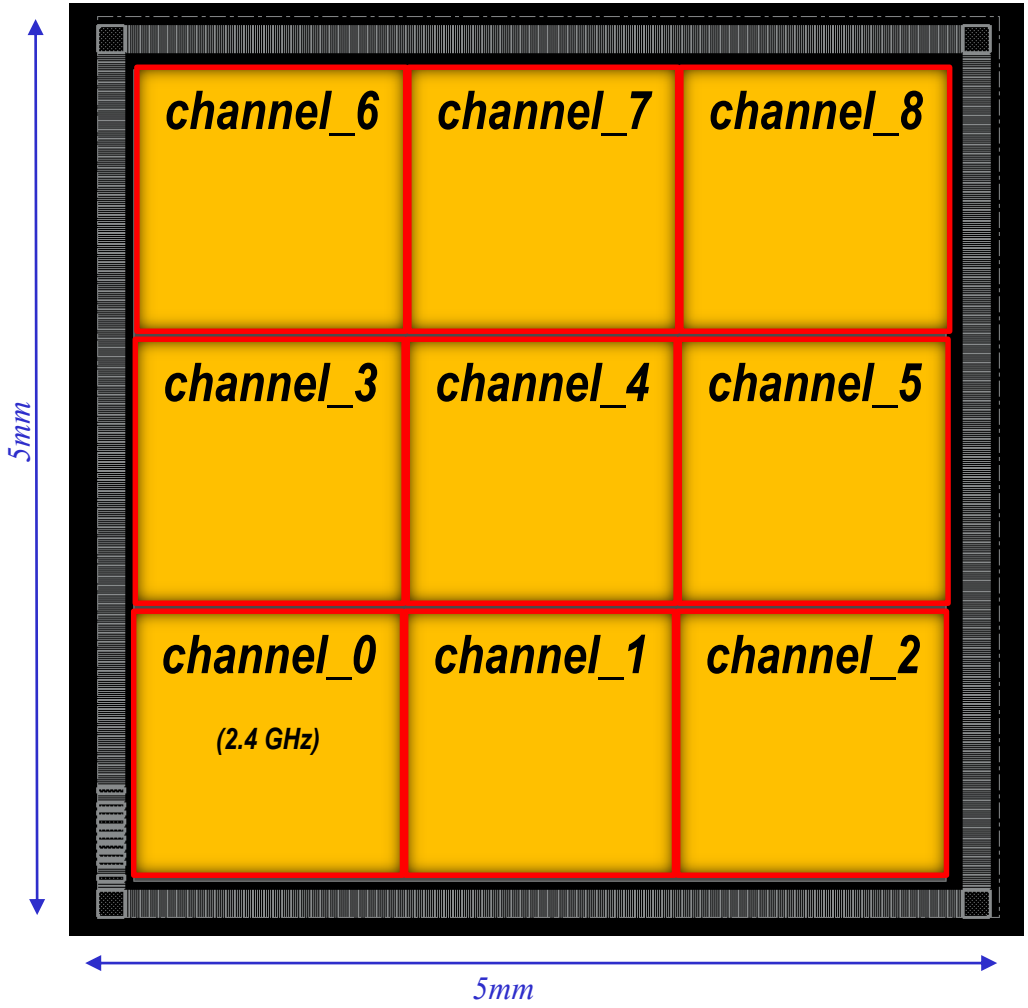
GPS correlator chip - floorplan



- Roughly 300,000 correlators on the same die (~**20M** std cells)

Power distribution concerns

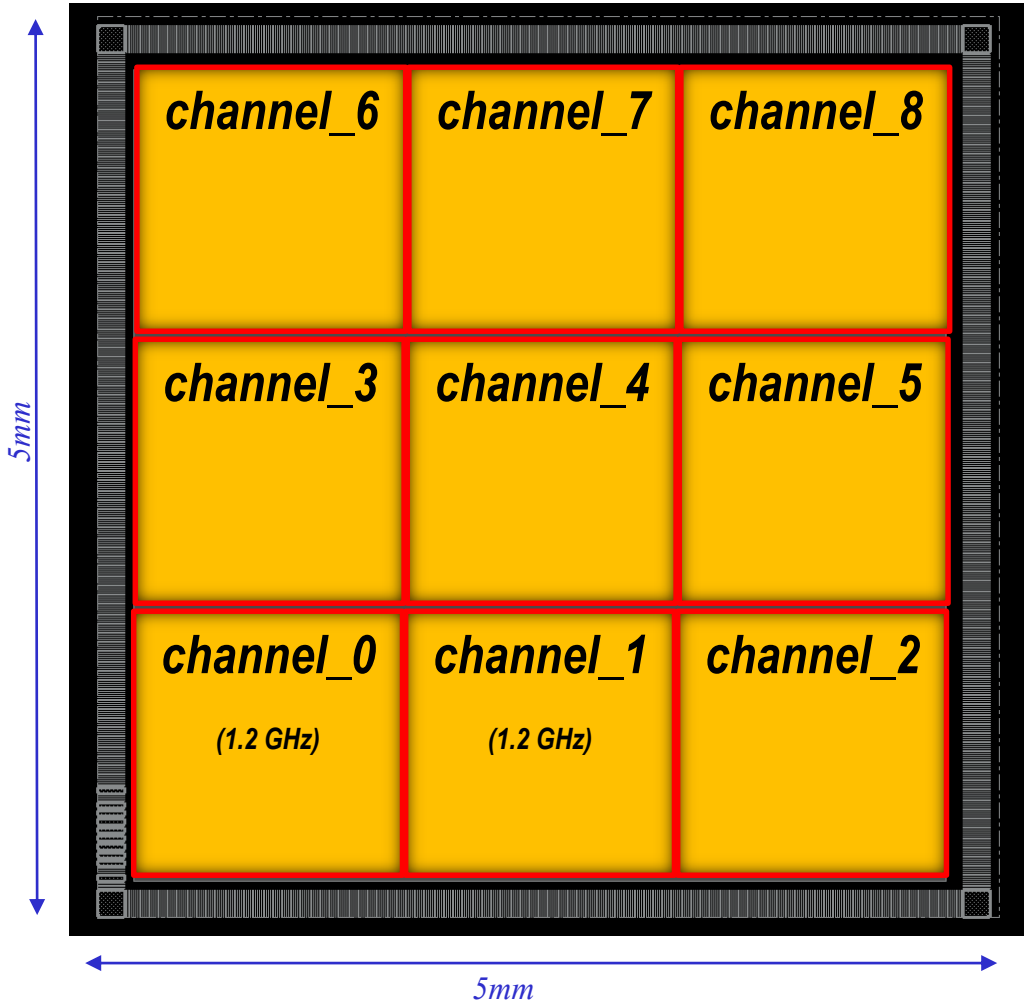
GPS correlator chip - floorplan



- Roughly 300,000 correlators on the same die (~**20M** std cells)

[config 1]

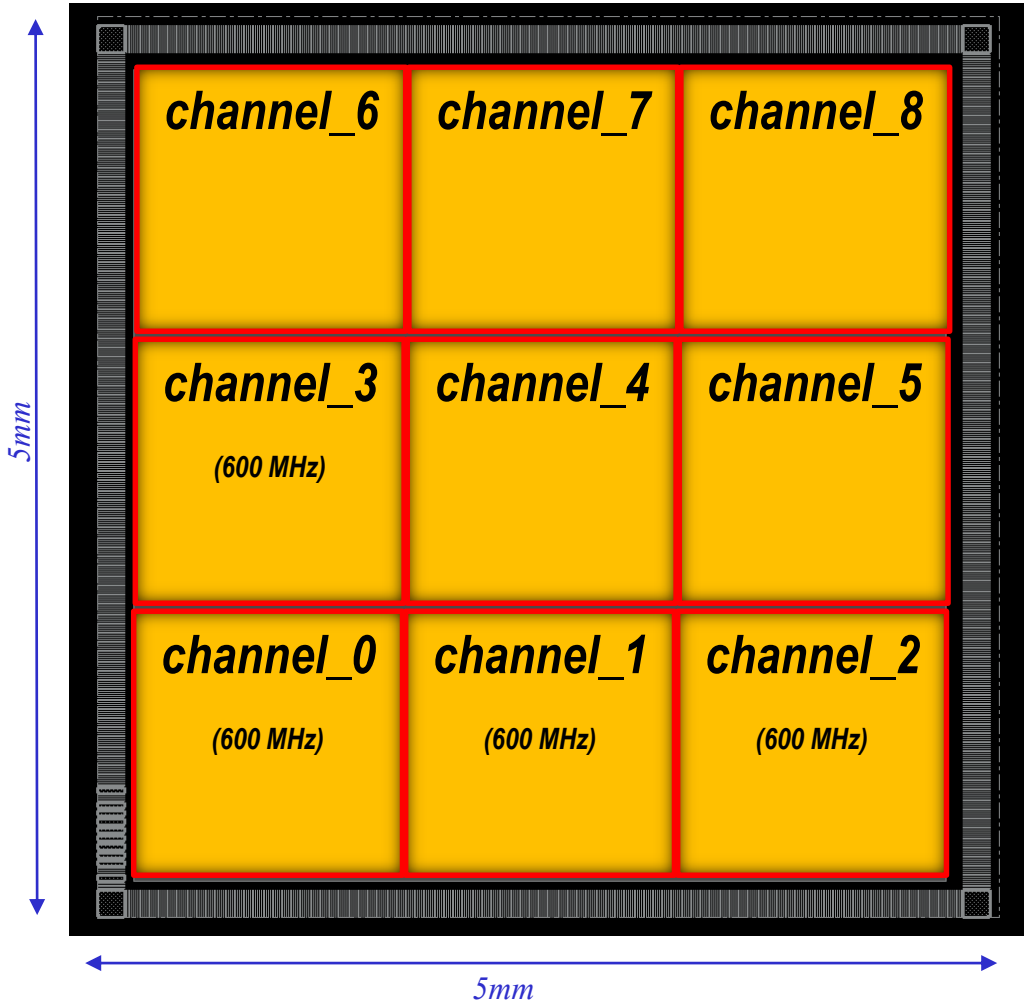
GPS correlator chip - floorplan



- Roughly 300,000 correlators on the same die (~**20M** std cells)

[config 2]

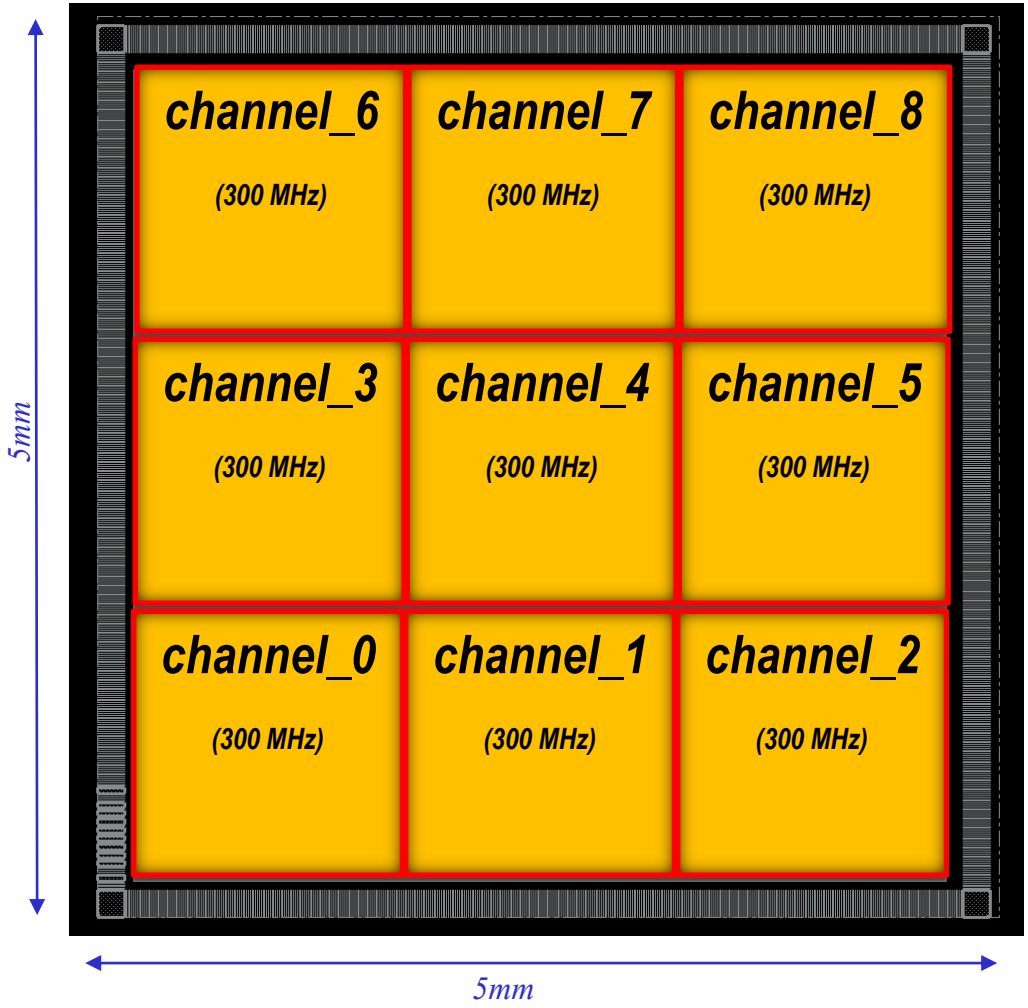
GPS correlator chip - floorplan



- Roughly 300,000 correlators on the same die (~**20M** std cells)

[config 3]

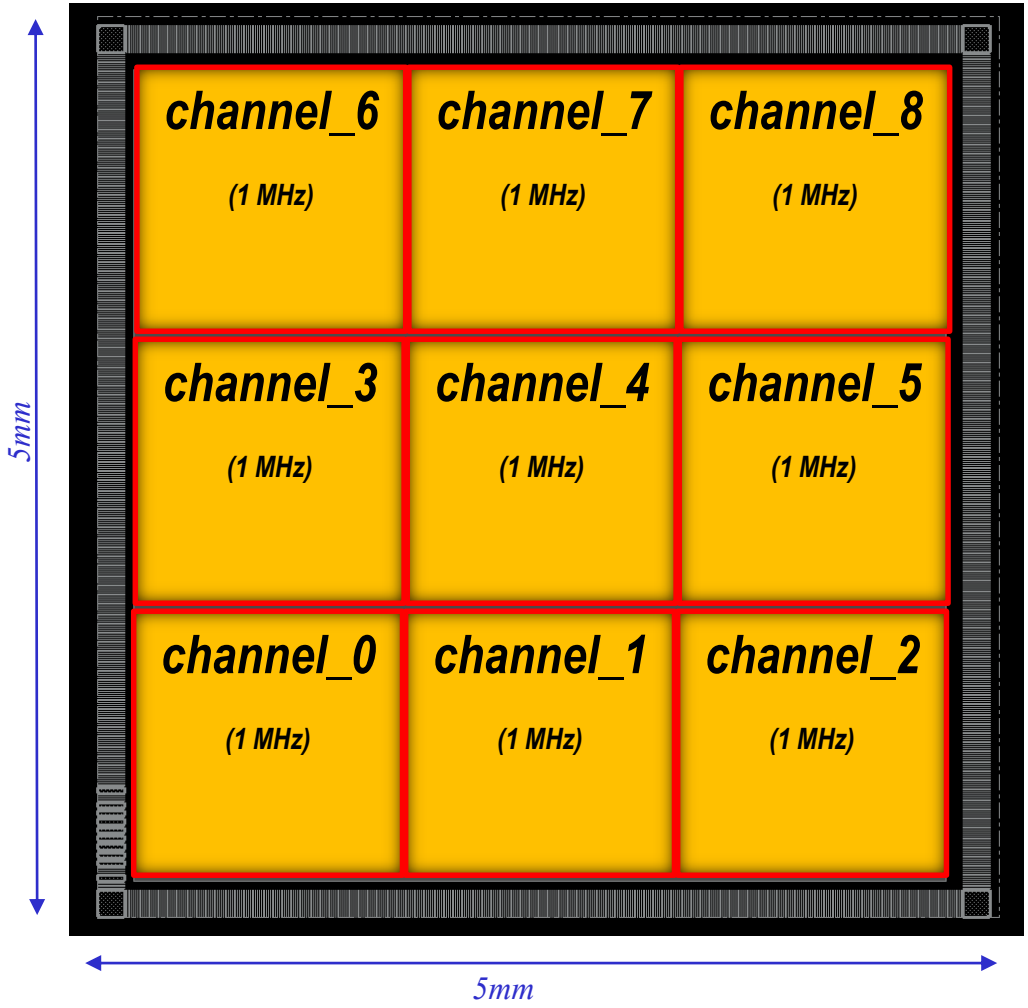
GPS correlator chip - floorplan



- Roughly 300,000 correlators on the same die (~**20M** std cells)

[config 4]

GPS correlator chip - floorplan

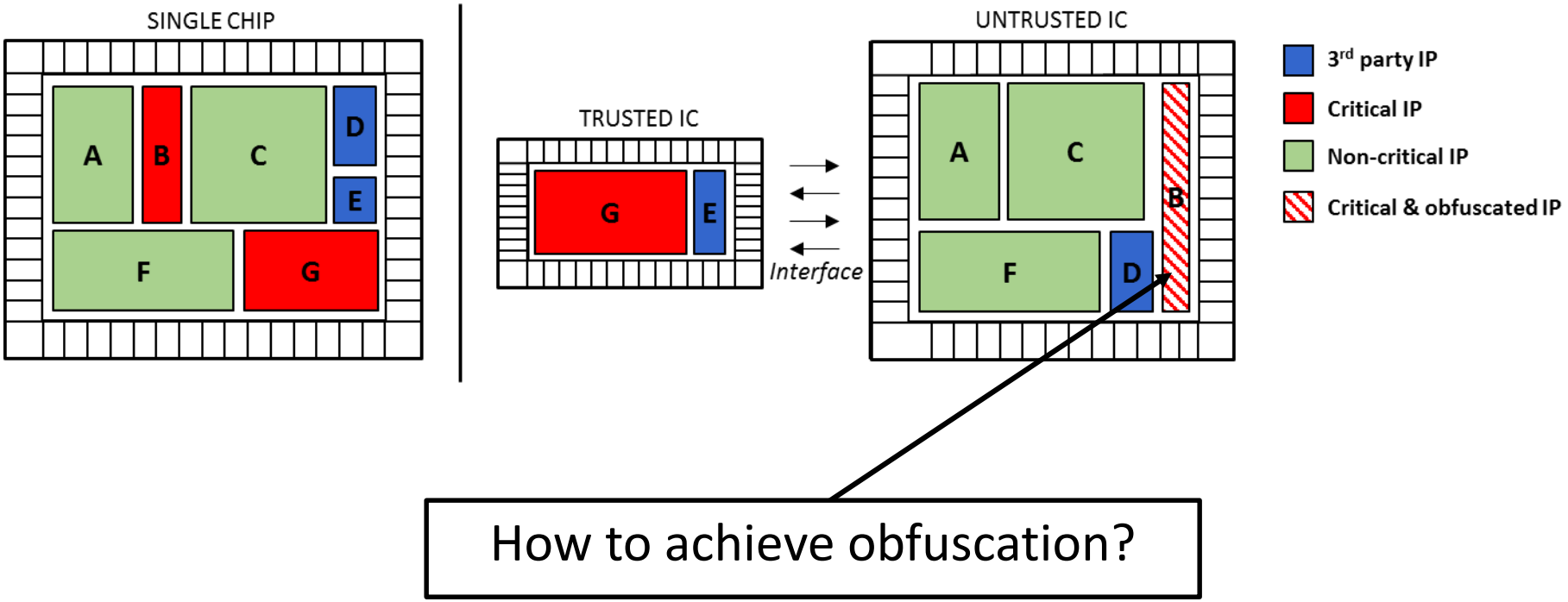


- Roughly 300,000 correlators on the same die (~**20M** std cells)

[config 5 – test/bringup only]

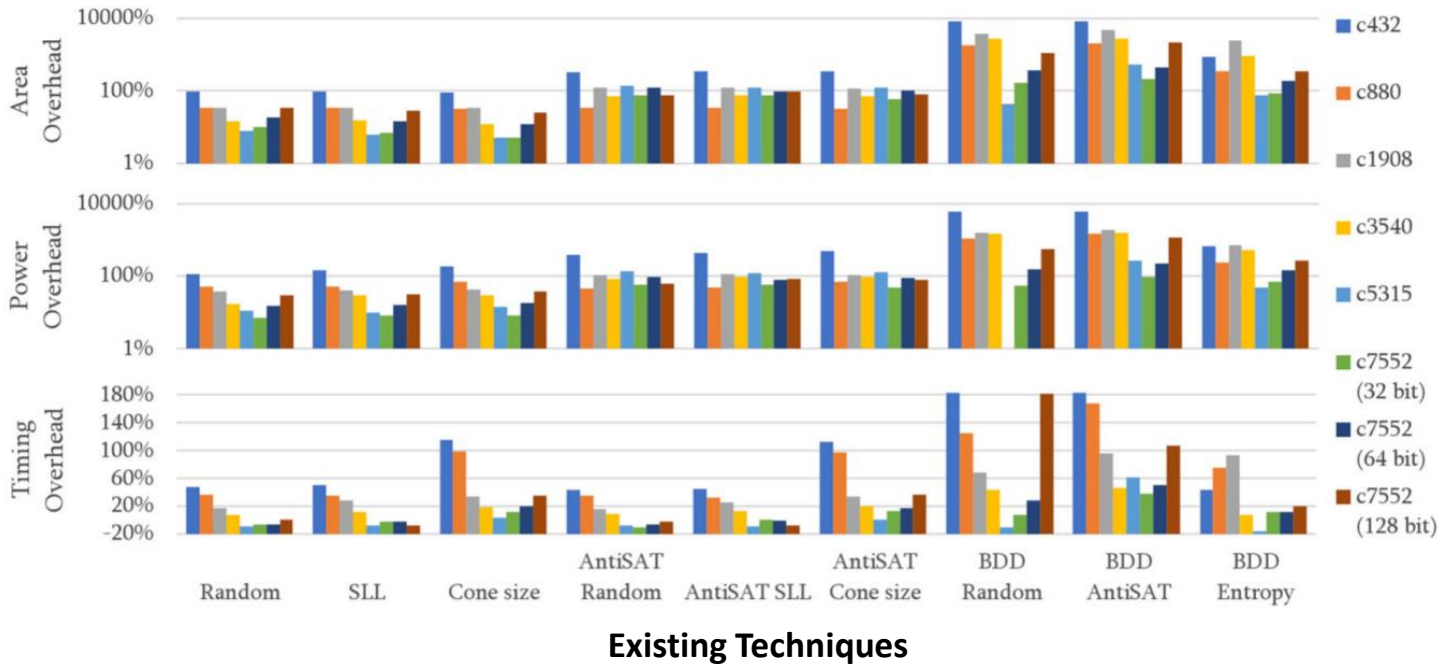
Split-Chip instead of Split-Fab

- Need for a CAD tool to assess the partitioning trade-offs
  - Technologies can be very different in nature
- Obfuscation schemes like keyed logic can be sought



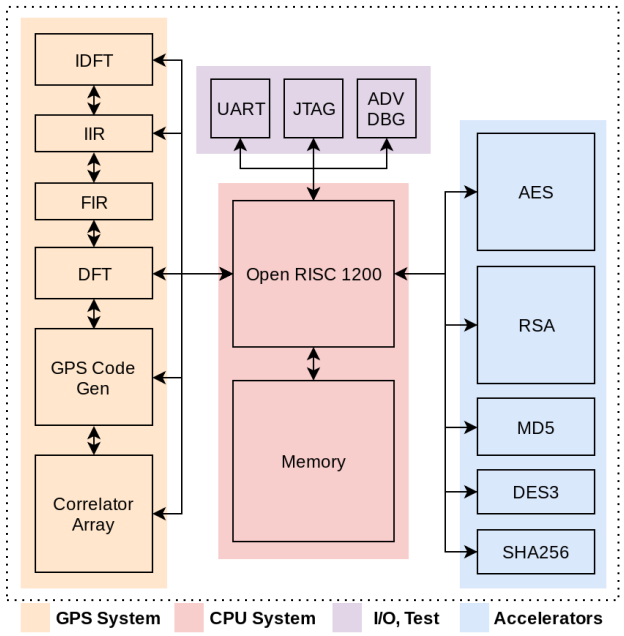
Obfuscation on Untrusted Chip

- **Modelled some existing logic locking techniques within the tool**
  - Vast literature available, several variants proposed



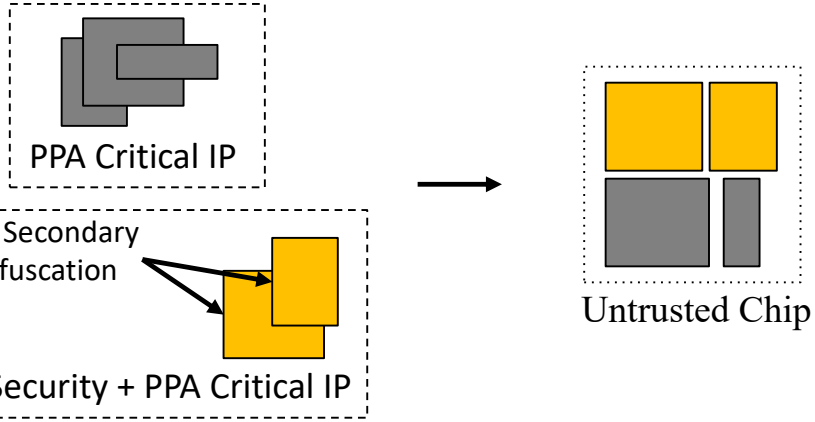
Amir, S., Shakya, B., Xu, X. et al. J Hardw Syst Secur (2018) 2: 142. https://doi.org/10.1007/s41635-018-0036-3

Split-Chip Design

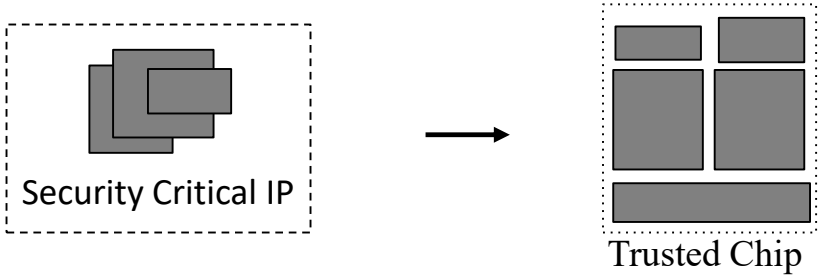


Original SoC

Advanced Node Untrusted Foundry



Legacy Node Trusted Foundry

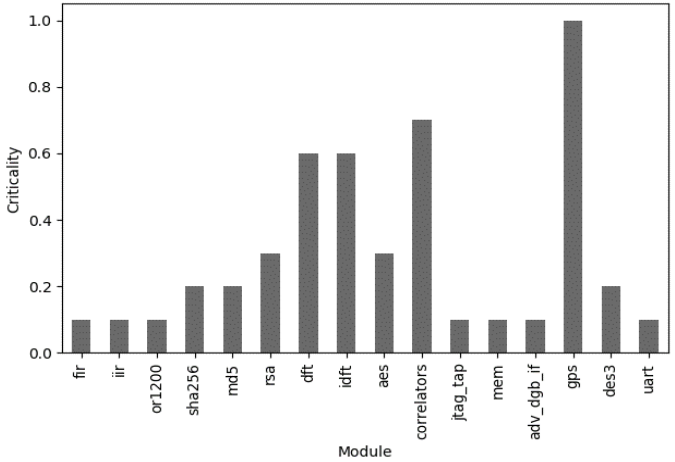


Vulnerability Optimization

X = {0,1,2,1,0,3, ...}
0: trusted
1: untrusted
2: untrusted, key logic
3: untrusted, FSM obf.

→ min f(**x**) = Vulnerability(**x**) = Exposure(C)*Criticality(M)
s.t. constraints met

Configuration	Exposure
Trusted	0.1
Untrusted	1.0
Untrusted w/ FSM Obf.	0.9
Untrusted w/ Keyed Logic	0.8



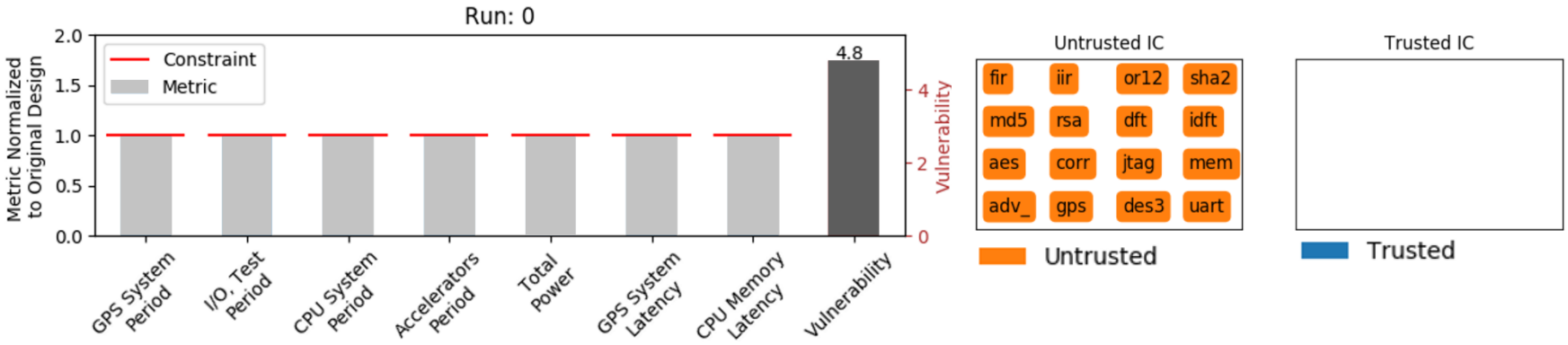
Technique exposure

- Ranks technique-related risk
- Score starts from 0 for maximal security on trusted chip

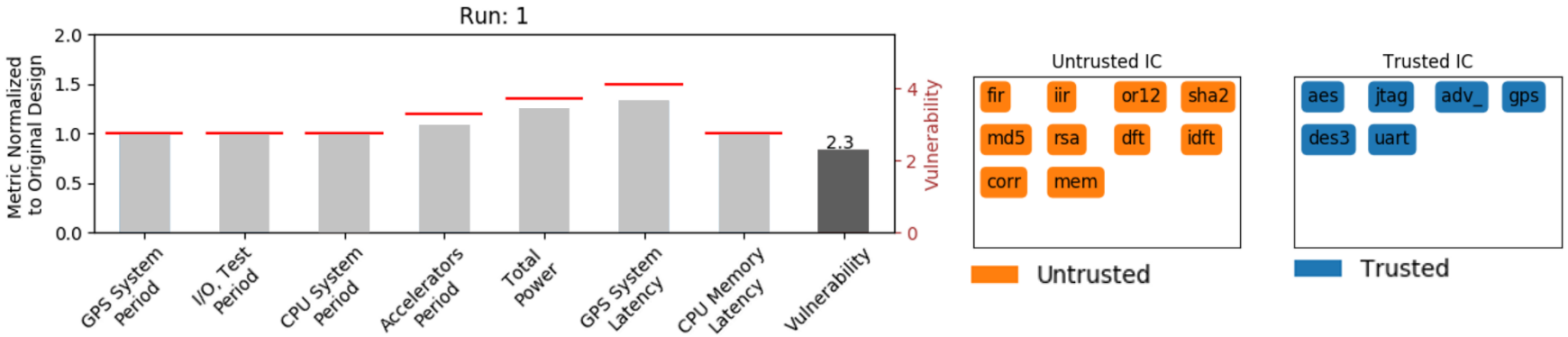
Module criticality

- User-defined scores
- Quantifies module risk/importance

Case study: Common Evaluation Platform

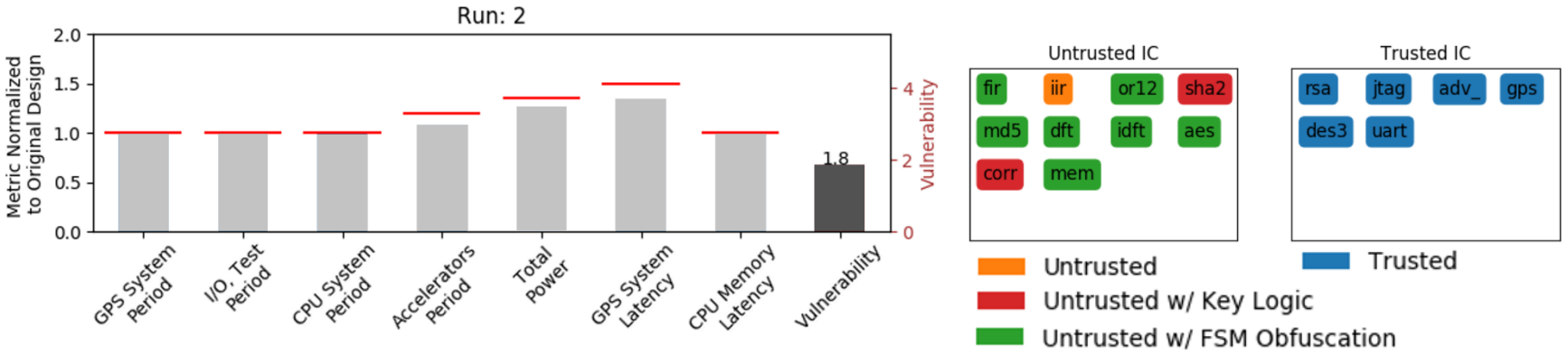


- No constraints relaxed from original design
- Fully on Untrusted IC w/ high vulnerability



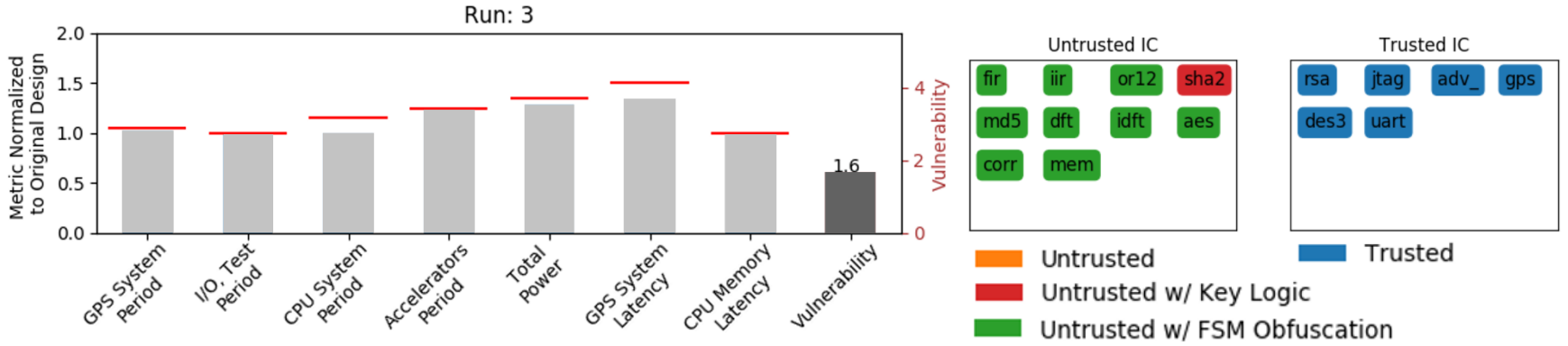
- Several constraints relaxed
- Significant decrease in vulnerability

Case study: Common Evaluation Platform



- Added keyed logic as secondary obfuscation to further reduce vulnerability

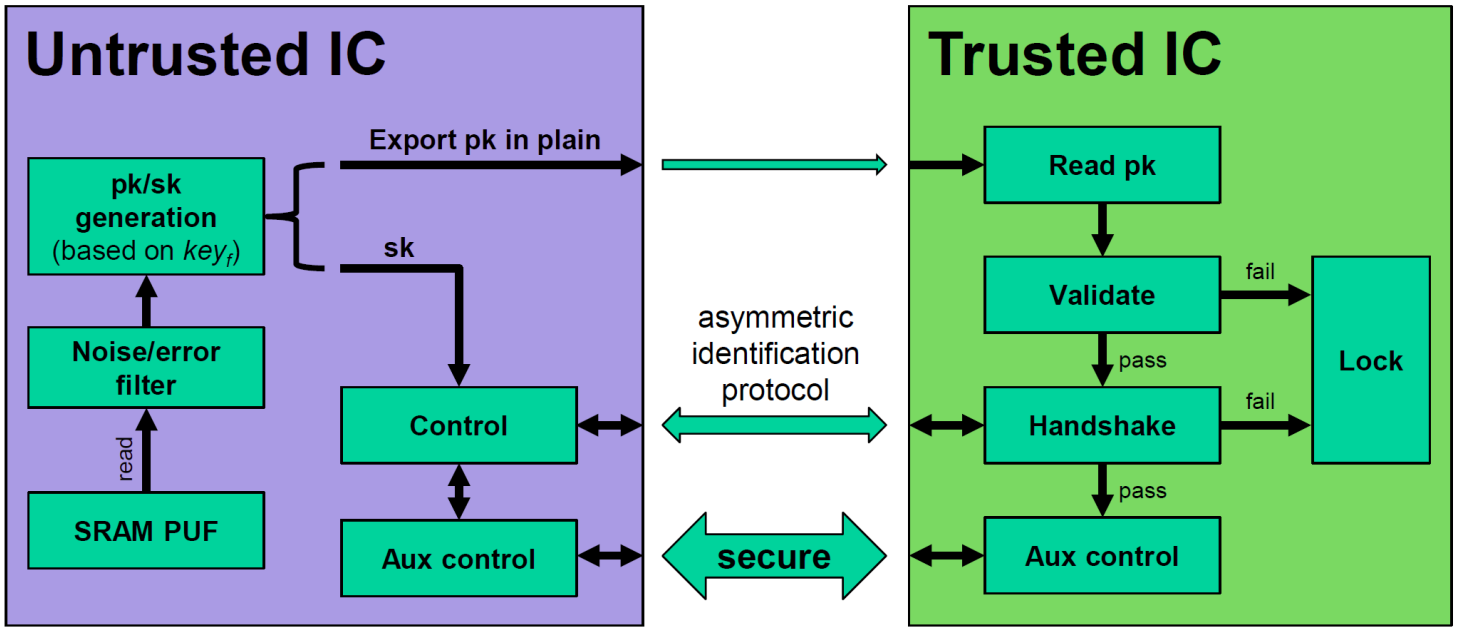
---



Manual observation: small tweak allows obfuscation on **every system module**

Pairing and encryption framework

- Uses SRAM as **signature** and asymmetric encryption (RSA)
- 1-to-1 pairing of Trusted and Untrusted ICs
  - Threats that are **unique to Split-Chip**
- Only **public key** is exchanged in the clear



Can we build a Trustworthy Billion Transistor Chip?

Carnegie Mellon University

Electrical & Computer ENGINEERING

We can build a Trustworthy-ish Billion Transistor Chip

How to measure trust?

Carnegie Mellon University

Electrical & Computer ENGINEERING

Lack of metrics

- Widespread problem for the hardware security community
- **Self-critical**: my interpretation of the state of the art

Configuration	Exposure
Trusted	0.1
Untrusted	1.0
Untrusted w/ FSM Obf.	0.9
Untrusted w/ Keyed Logic	0.8

Thanks!

Carnegie Mellon University

Electrical & Computer ENGINEERING