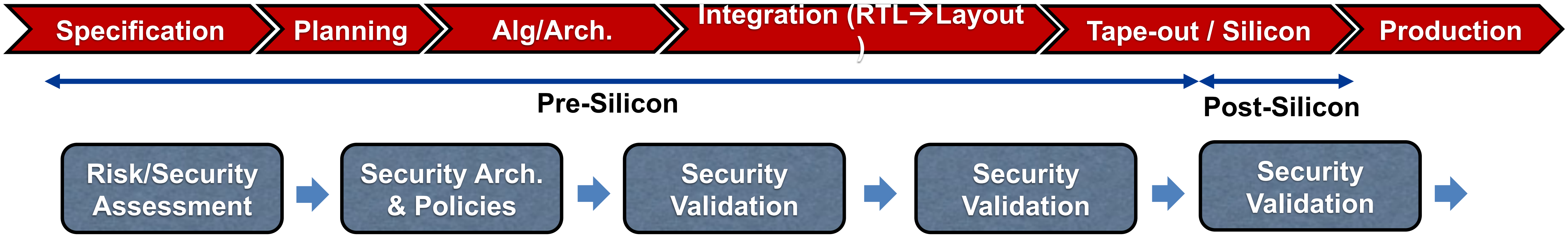
Security Verification:
From High Level Design to Physical Layout

Mark M. Tehranipoor

Sachio Semmoto Chair, ECE Department
Intel Charle E. Young Endowed Chair Professor

UNIVERSITY *of* FLORIDA

SDL: Security Development Lifecycle



Risk Assessment
Includes definition of assets, threat model, adversaries, and security policies

Secure Architecture
Threat Modeling; Define architecture support for security; Review architecture level security Policies

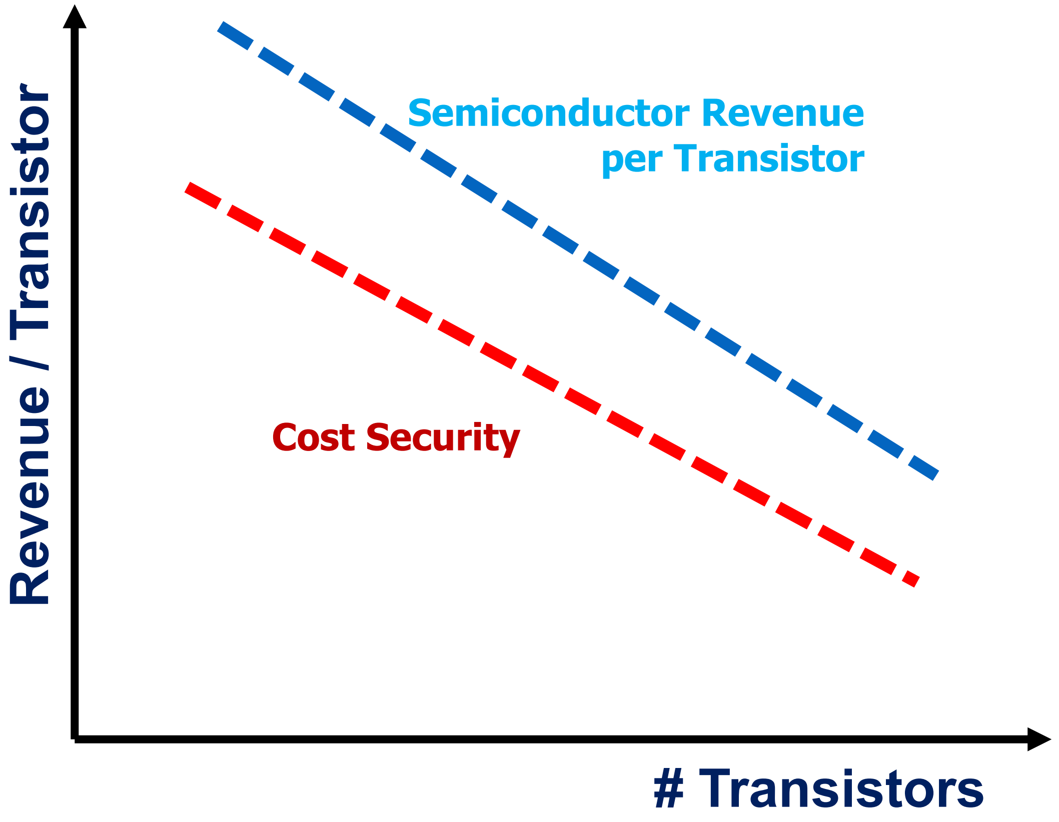
Pre-silicon Security Verification:
Threat Modeling; Design review; Security verification against attacks at different stages of the design process;

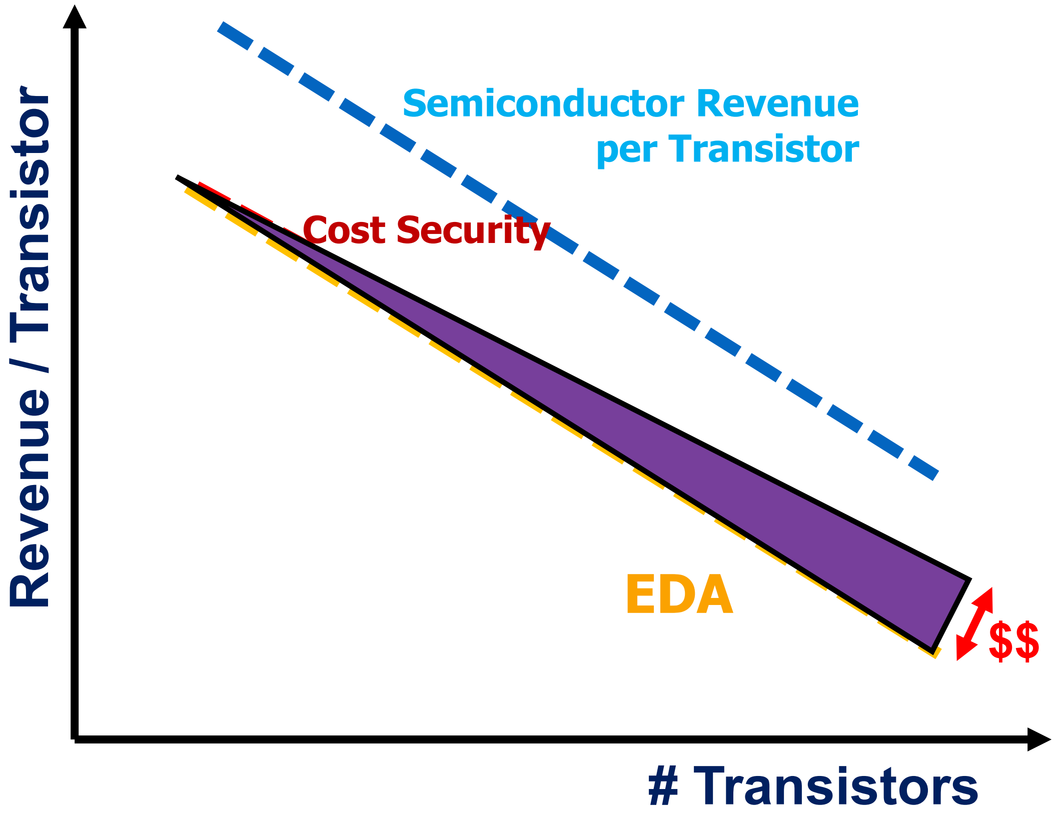
Post-Silicon Security Verification:
Fuzzy test, Negative test, and penetration test

Offered by Caspia Technologies – www.caspiatehnologies.com

Need Automation

PASS:
Power, Area, Speed, Security



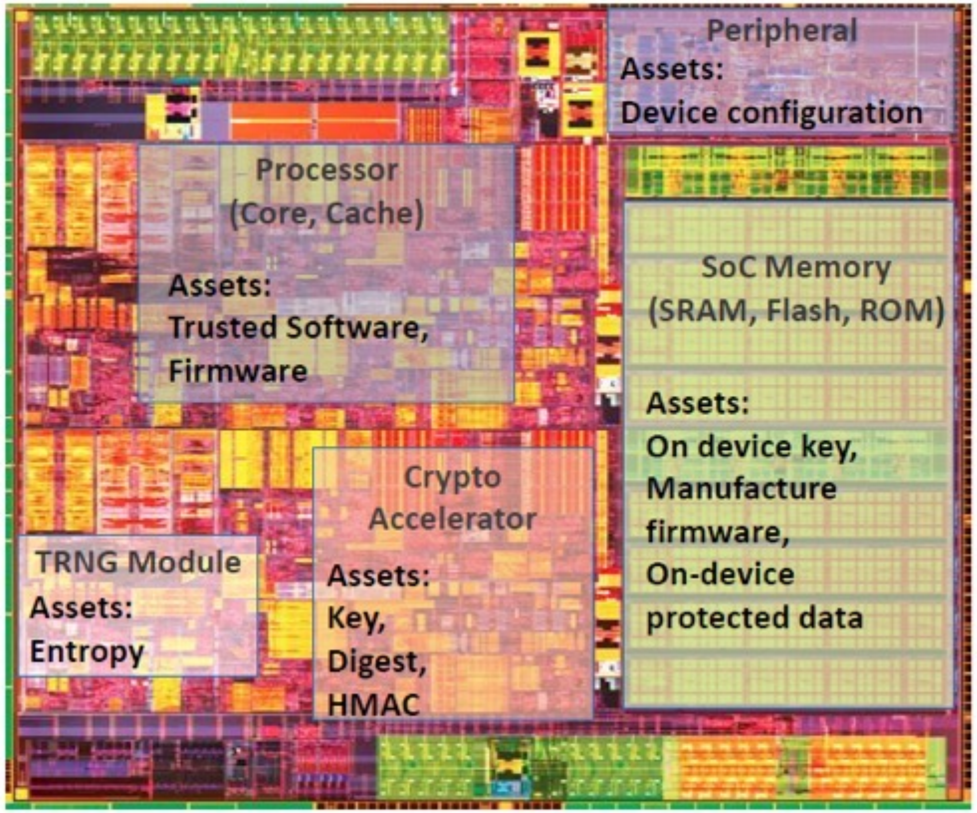


Challenges: Security Assets

Asset: A resource of value worth protecting from an adversary

Security Assets in SoCs:

- On-device keys (developer/OEM)
- Device configuration
- Manufacturer Firmware
- Application software
- On-device sensitive data
- Communication credentials
- Random number or entropy
- E-fuse,
- PUF, and more…



Source: Intel

Challenges: Vulnerabilities - Growing

- Fault Injection
- Privilege Escalation
- Trojan Insertion
- Trace Buffer
- EM Side-Channel
- CLKSCREW
- Denial-of-Service
- Vector Rewrite
- Rowhammer
- Power Side-Channel
- Direct Memory Access
- BranchScope
- Bitstream Encryption Cracking

- Plundervolt
- Access Control
- Meltdown and Spectre
- Machine Learning
- Information Leakage
- Trusted Execution Environment Breaking
- Reset and Flush
- Branch Shadowing
- Bitstream Tampering
- Reverse Engineering
- Timing Side-Channel
- Integrity

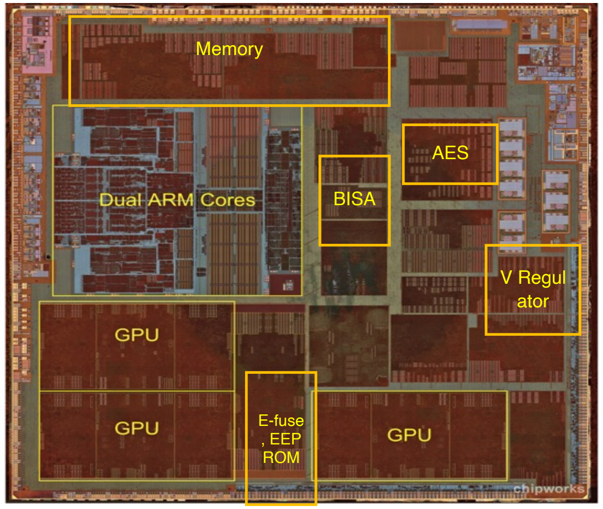
People: the weakest link!

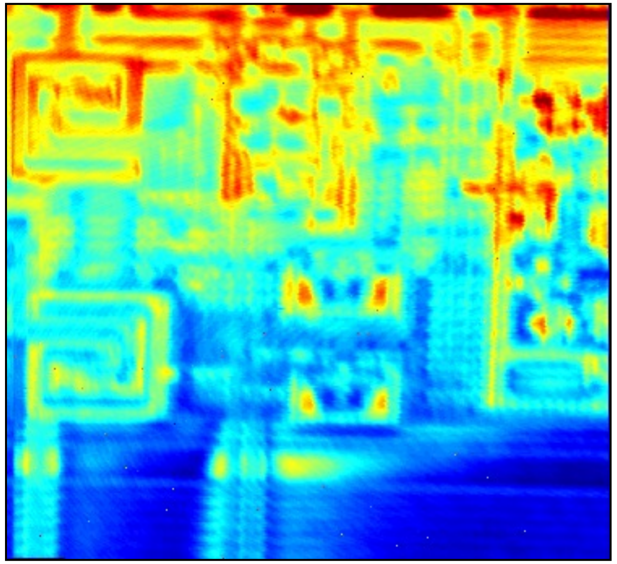
Strong Algorithm & Architecture

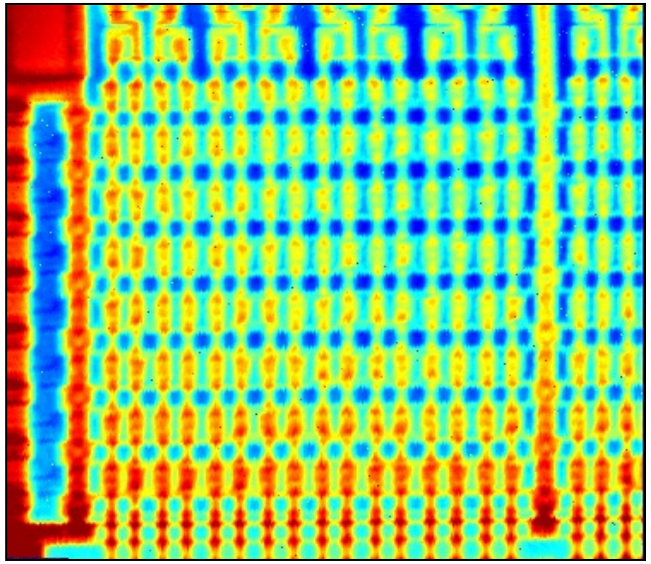
Weak Implementation & Execution

Unique to Physical Layout

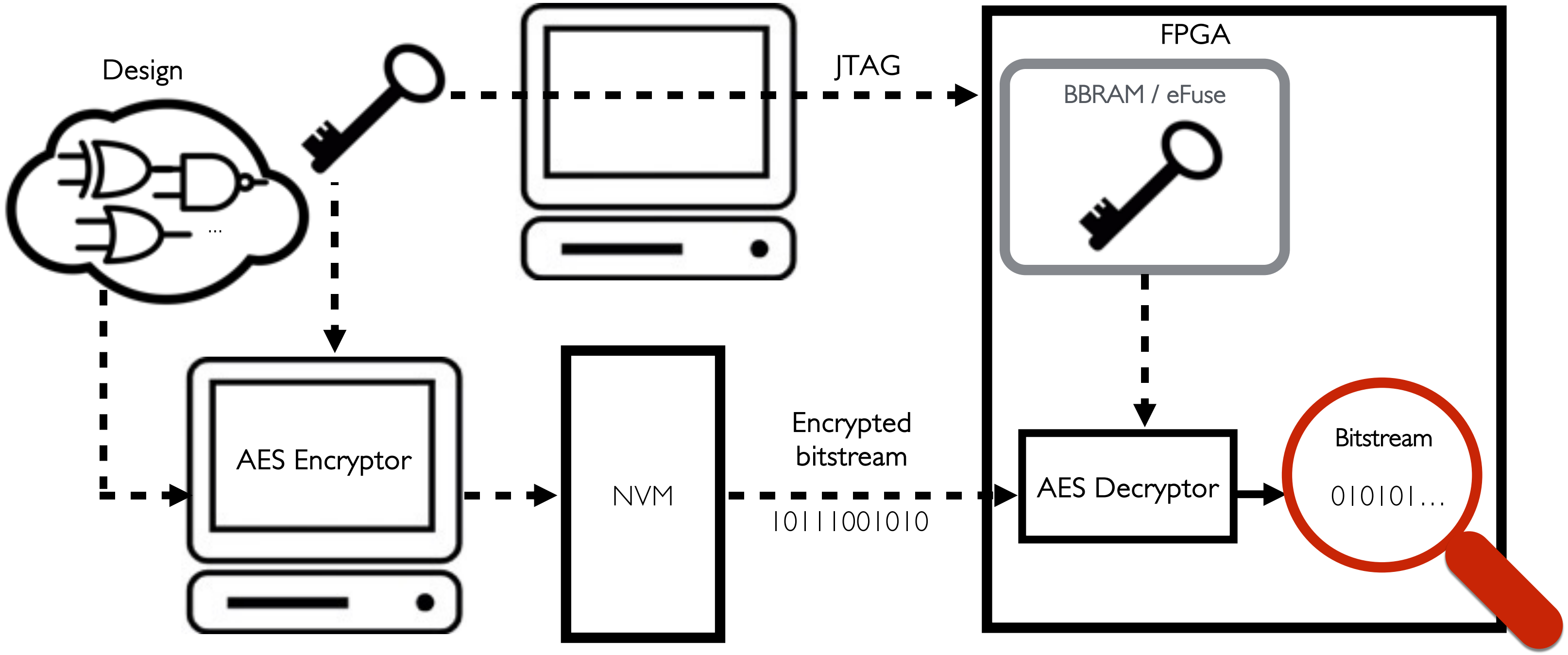
- **Protect against untrusted foundry**
- **Address IP piracy**
  - Physical Locking
- **Protect crypto cores**
  - Power side channels; EM Side channels; Fault injection
- **Protect physical attacks**
  - Contactless probing attacks; Contactless optical attacks; Laser fault injection attacks; X-ray attacks; Electromigration



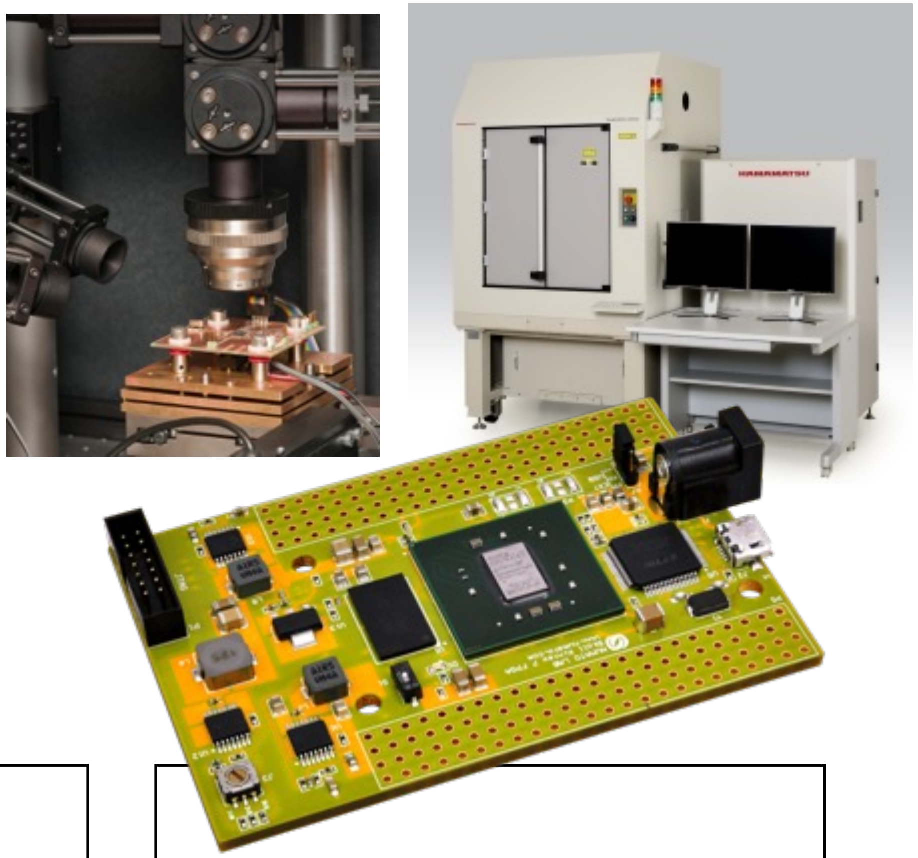




Chip Backside Is A New Backdoor



Hamamatsu PHEMOS - 1000



- Device under Test (DUT): Xilinx Kintex 7 development board
  - Chip's technology: 28 nm
  - No chip preparation (e.g., depackaging, silicon polishing, etc.)
- Optical Setup: Hamamatsu PHEMOS-1000
  - Laser wavelength: 1.3 μm
  - Laser spot size: >1 μm

- Non-destructive
- Non-invasive
- No Footprint

Localizing the Configuration Logic

Xilinx Kintex 7 in flip-chip package

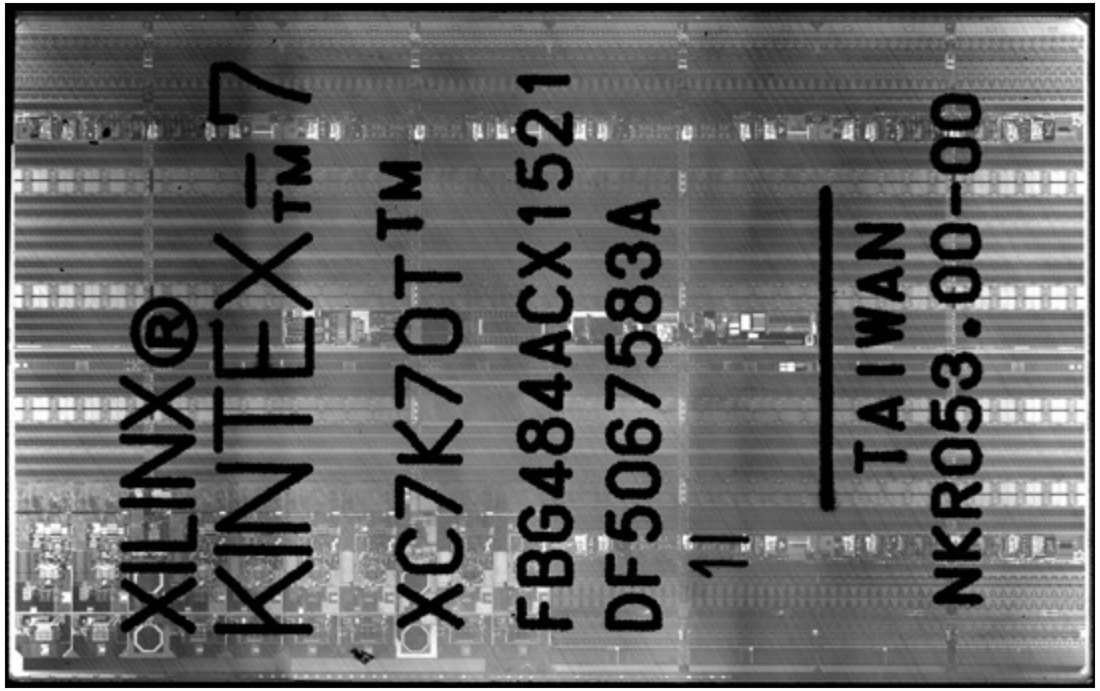
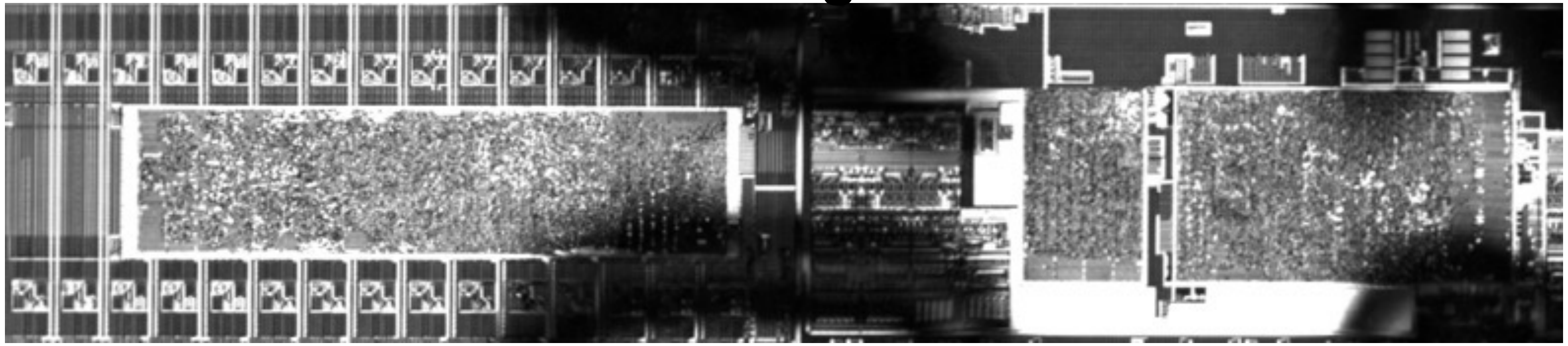


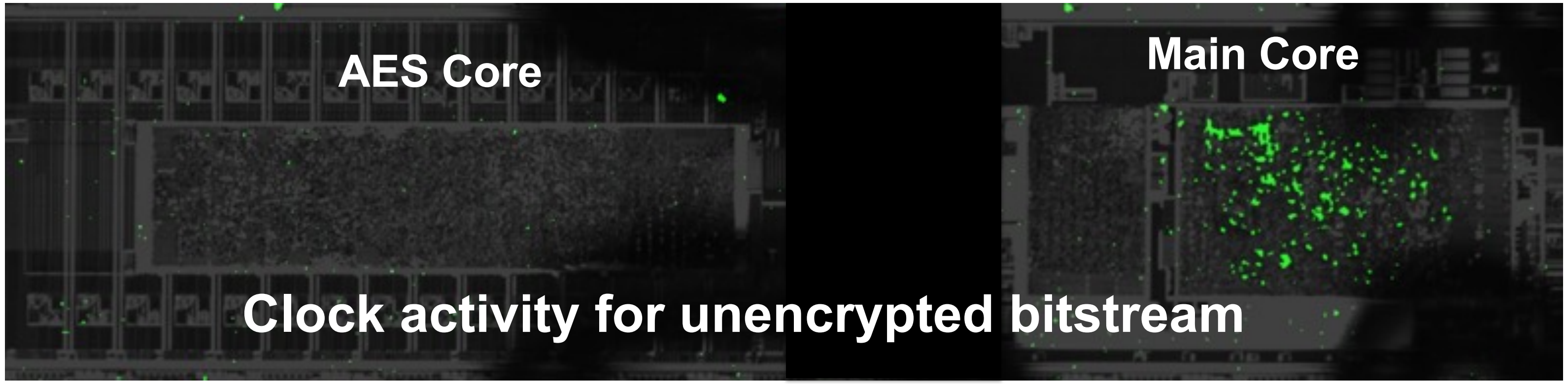
Image acquisition with a infra-red laser scanning microscope

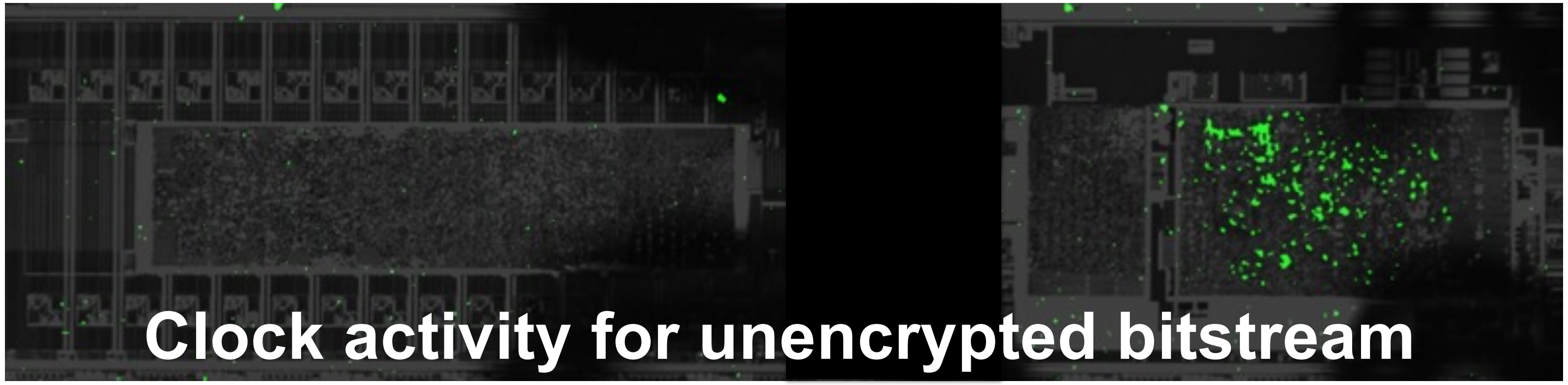
Tajik, S., Lohrke, H., Seifert, J. P., & Boit, C. "**On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs**," In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.

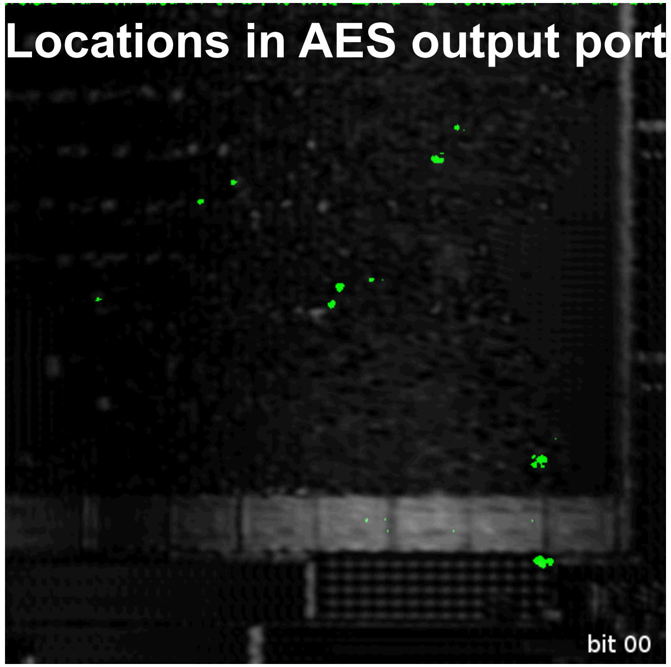
Localizing Decryption Engine

Random Logic

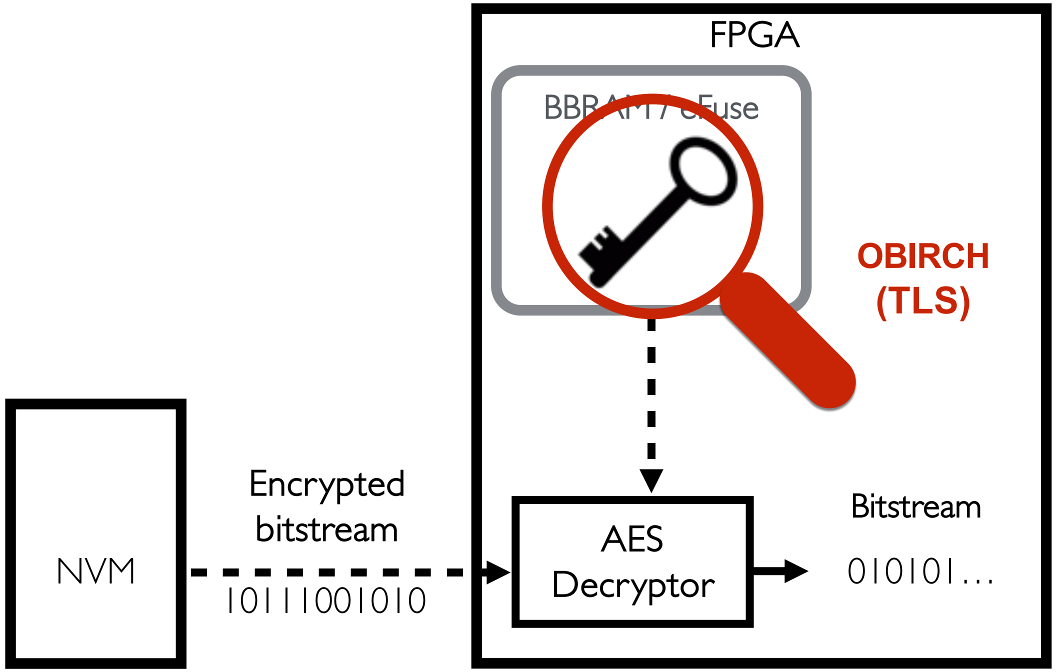


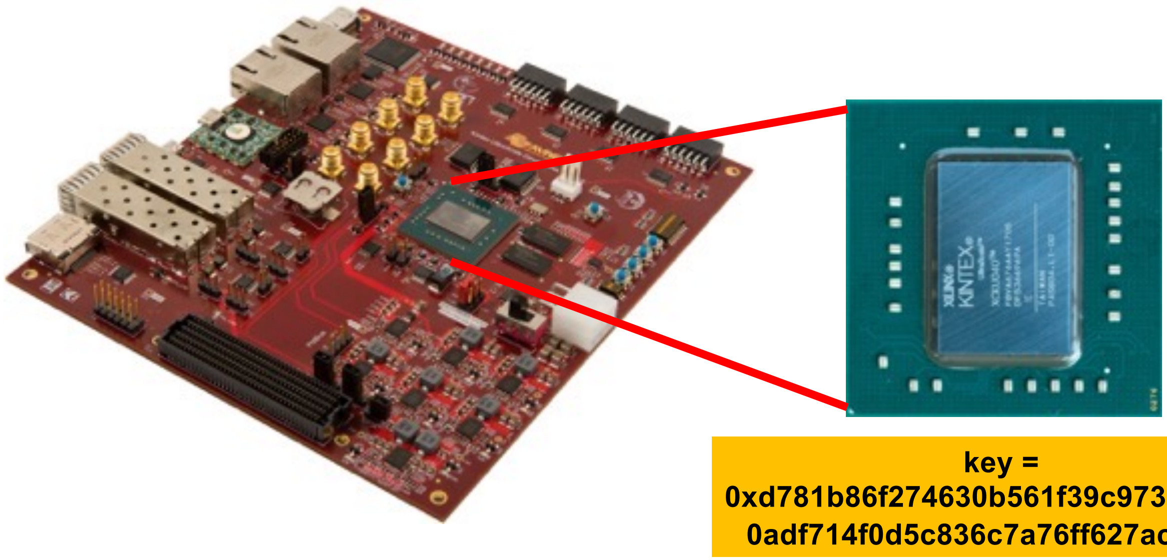






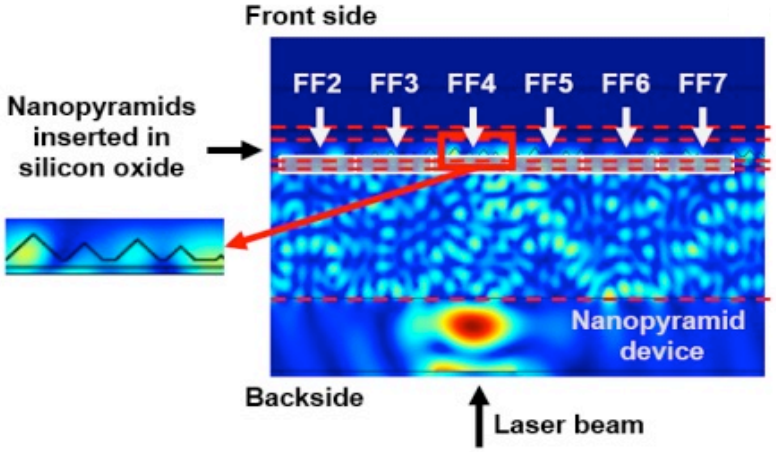
Key Extraction

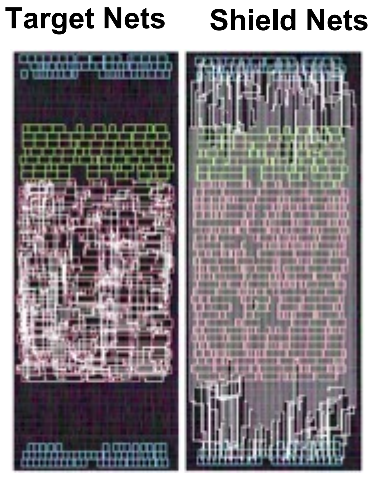




key = 0xd781b86f274630b561f39c9736f512eb 0adf714f0d5c836c7a76ff627aca4923

- **Protection**
  - **Circuit Level Solutions**
  - **Device Level solutions**
  - **Material Level Solutions**





?