All Programmable System on Chip Security

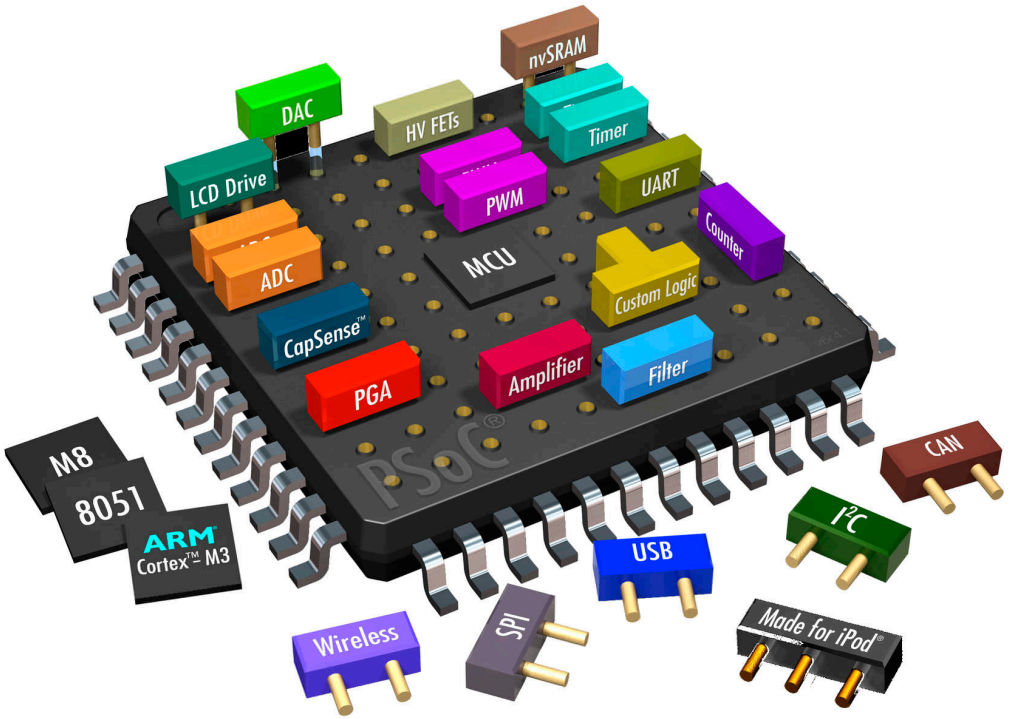
Presented by
Amit Singh

Outline

- Introduction
- Salient features of Zynq-7000 & SmartFusion2
- Features:
  - Crypto implementations & key loading
  - Storage & security during operations
  - Product lifecycle
- Key similarities & differences
- Summary

Introduction

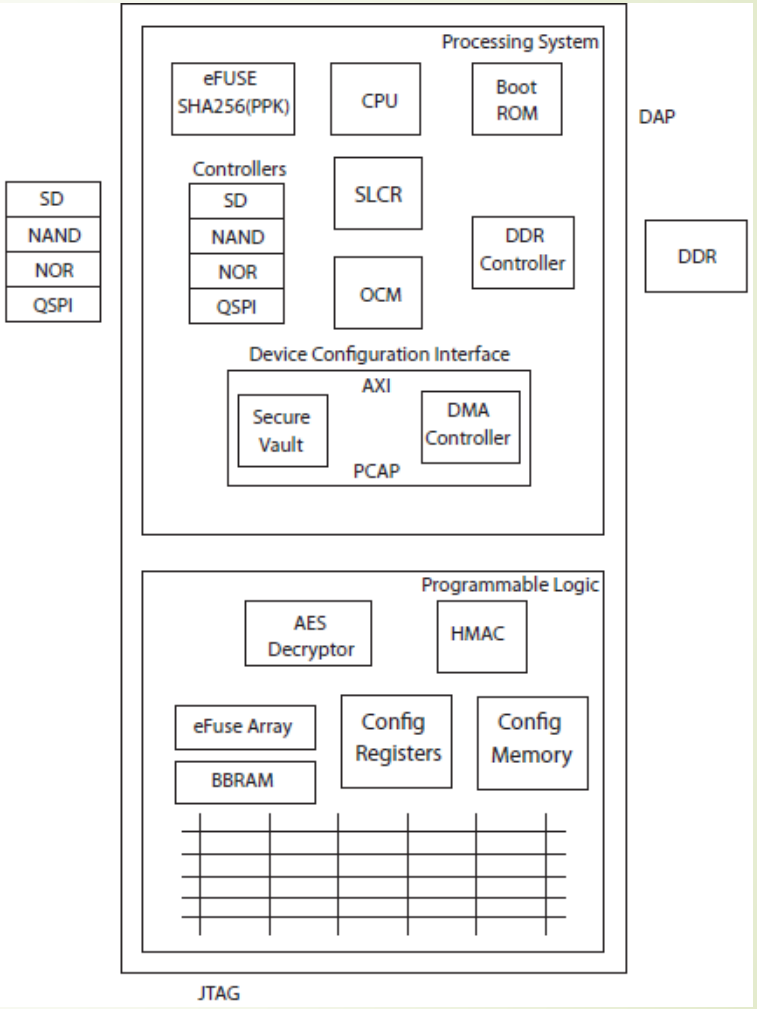
- What is *system on chip*?
- Why are they important?
- Goal of this project



Source "PSOC" url: http://www.directindustry.com/prod/cypress-semiconductor/product-34220-200113.html

Zynq-7000 by Xilinx

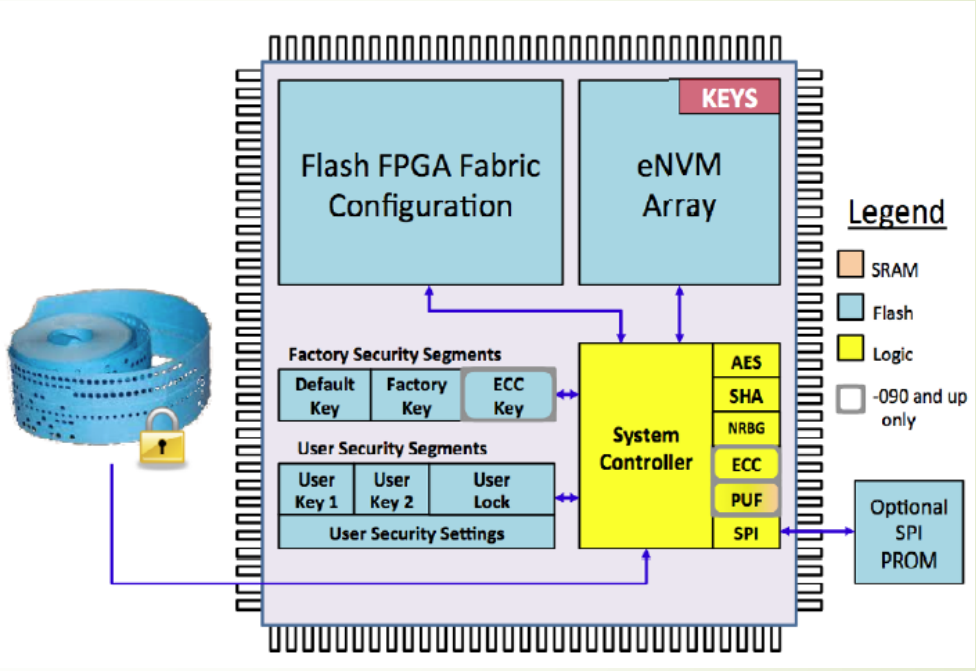
- 2 parts:
  - Processing system (PS)
  - Programmable logic (PL)
- Memory storage
  - Boot ROM
  - On-chip memory
  - Configuration memory
  - Other memories
- Cryptographic block
  - AES decryptor, HMAC (embedded in hardware)
  - RSA (embedded in software)



Source : xapp1175_zynq_secure_boot by Lester Sanders in 2015

SmartFusion2 by Microsemi

- Similar to Zynq-7000
  - Microcontroller subsystem
  - FPGA fabric
- Memory storage
  - Flash
  - SRAM
  - PROM
  - Other memories
- System Controller (Crypto)
  - AES, HMAC-SHA-256, ECC
  - PUF, NRBG



Source : Basic Design Configuration Programming by G. Richard Newell, Security Forum, 2012

Outline

- Introduction
- Salient features of Zynq-7000 & SmartFusion2
- **Features**:
  - Crypto implementations & Key loading
  - Storage & security during operations
  - Product lifecycle
- Key similarities & differences
- Summary

Features based on Crypto implementations & Key loading

Zynq-7000

- Advanced Encryption Standard (AES) & Secure Hash function-256 (SHA-256)
- RSA algorithm
- Hardware security module
- Keys are loaded by developer
- Hashed key storage

SmartFusion2

- Advanced Encryption Standard (AES) & Secure Hash function-256 (SHA-256)
- Elliptic Curve Cryptography (ECC) & Non-deterministic random number generator (NRBG)
- Hardware security module
- Initially, developer keys, loaded by manufacturer
- Hashed key stored

Features based on Storage & Security during operation

Zynq-7000

- Unencrypted storage
- Security sensitive codes stored on-chip
- Key storage options:
  - eFUSE (One-time programmable)
  - BBRAM (Volatile)
- Key update

SmartFusion2

- On-the fly encryption/decryption
- Security sensitive codes stored in encrypted form or at least hash copy on-chip
- Key storage options:
  - Flash memory (non-volatile)
  - BBRAM, eFUSE
- Key update
- Randomization in data encryption

Features based on Product lifecycle

Zynq-7000

- Immutable boot ROM code
- Using sequence number for partitions
- Anti-tamper measures
  - Lockdown mode
  - PS-PL monitoring

SmartFusion2

- Immutable bootloader code
- Using sequence number for partitions
- Anti-tamper measures
  - Penalty
  - Security mesh, User service Interface (USI)
  - Zeroization
- Certificate revocation list

Outline

- Introduction
- Salient features of Zynq-7000 & SmartFusion2
- Features:
  - Crypto implementations & Key loading
  - Storage & security during operations
  - Product lifecycle
- **Key similarities & differences**
- Summary

Key similarities

- Similar Cryptographic ciphers (except RSA vs ECC)
- Multistage boot loading
- Initial stage immutable
- Sequence numbers for each partition
- Hashed keys

Key differences

- Zynq-7000 (Z7) supports only decryption vs SmartFusion2 (S2) supports both encryption/decryption
  - S2 supports hardwired NRBG
  - S2 supports modes of operation (ECB, CBC)
- Z7, runs First stage boot loader (FSBL) code vs S2 uses hardwired system controller
- S2 supports in fab installation of user settings vs Zynq has no such facility
- Additional features supported by S2
  - Physical Unclonable function
  - Zeroization, Certificate revocation list

Summary

- SmartFusion2:
  - Elaborated key handling
  - Better implementation of security services
  - Root of trust features
- Zynq-7000:
  - Simplistic approach
  - Less time to market
- Overall security features
  - SmartFusion2 leads (on the fly encryption & decryption, PUF & other features)

Summary

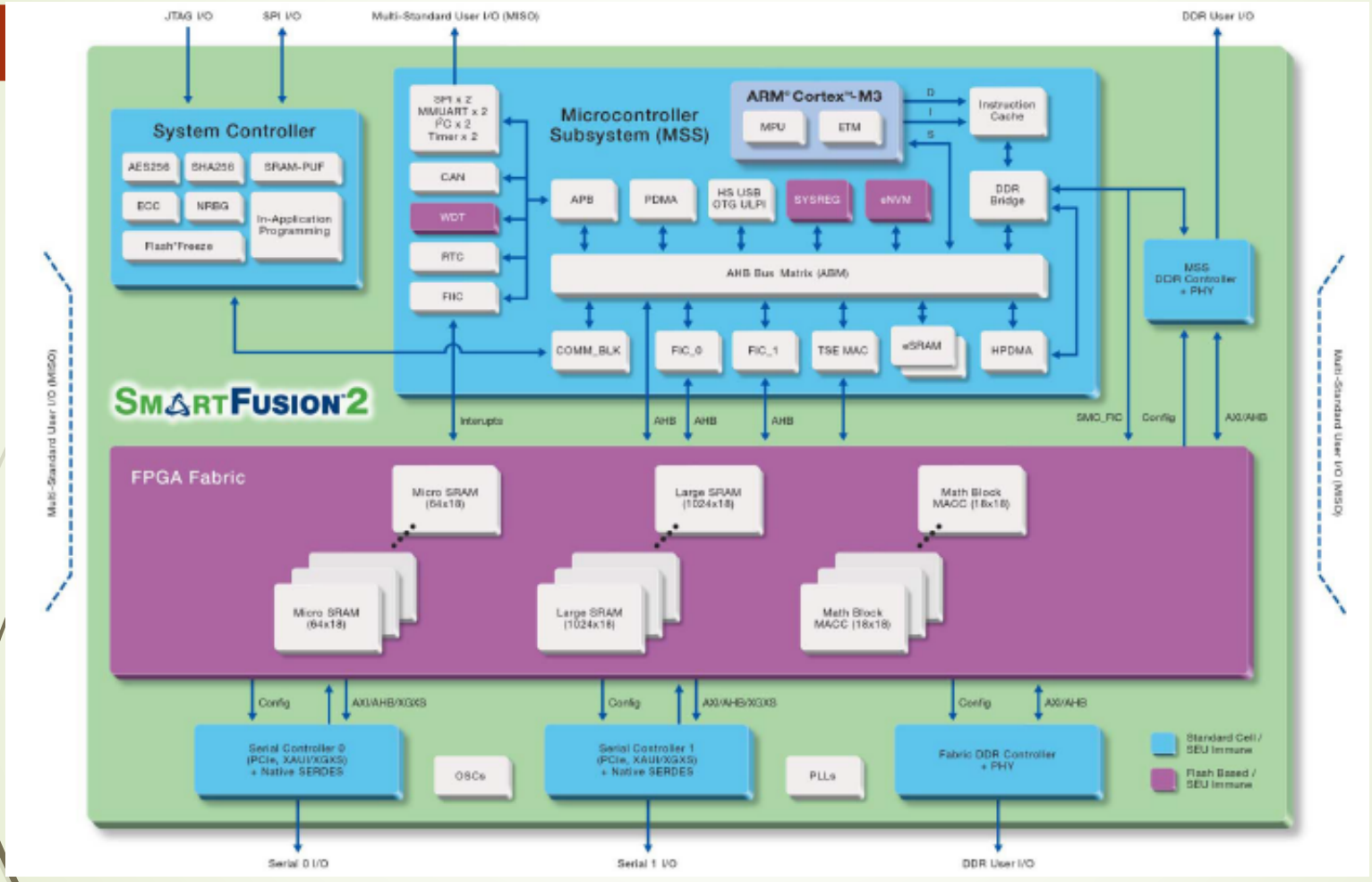
- Security features essential in modern SoC:
  - On the fly encryption/decryption
  - ECC, AES, SHA, NRBG
  - PUF for device id
  - SRAM-PUF for key generation
  - Hashed keys
  - Partition sequencing
  - Zeroization

Thank you

Any Questions?

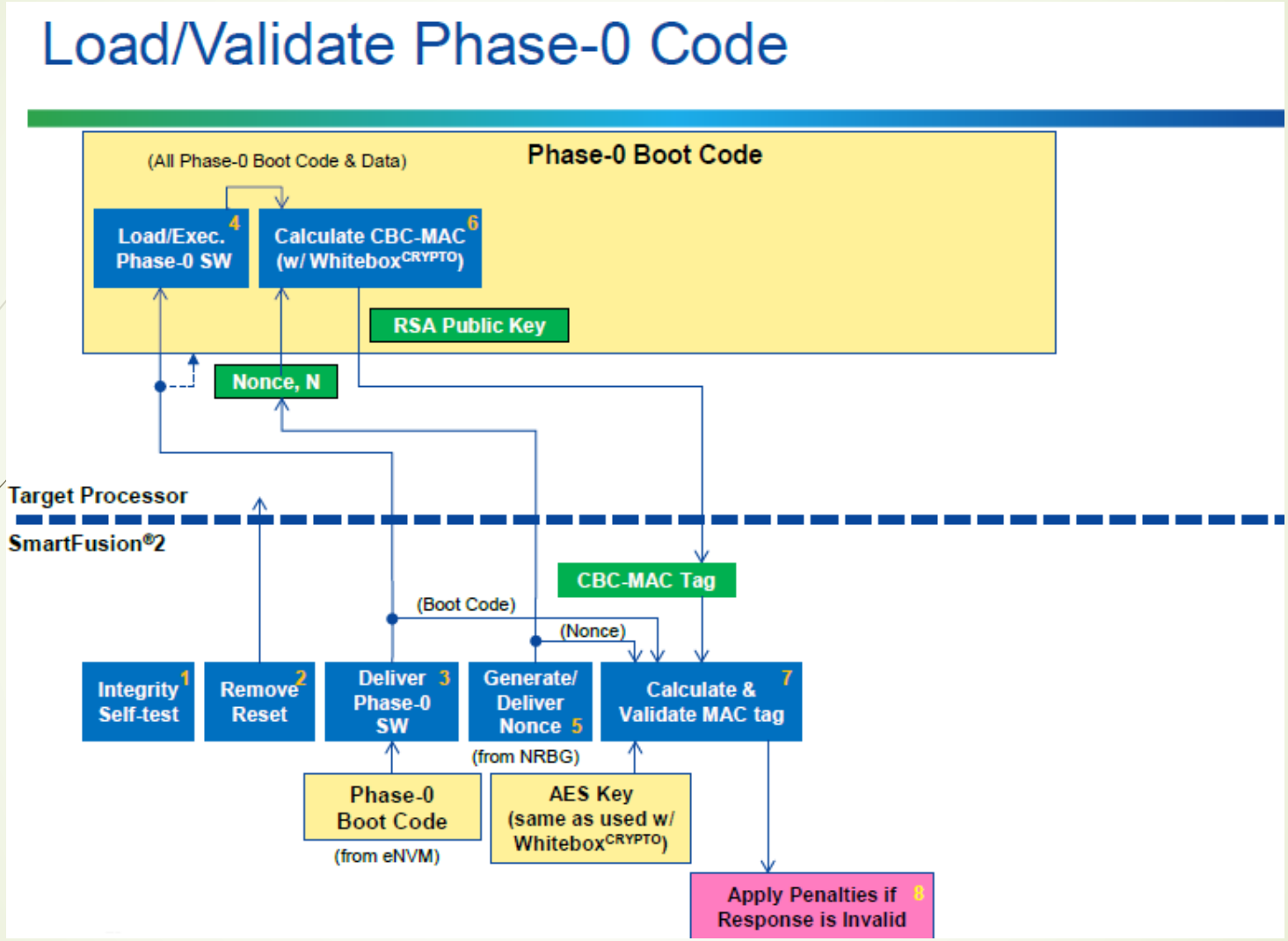
Backup slides

SmartFusion2 architecture



Source : Overview of Secure Boot, Microsemi, 2013

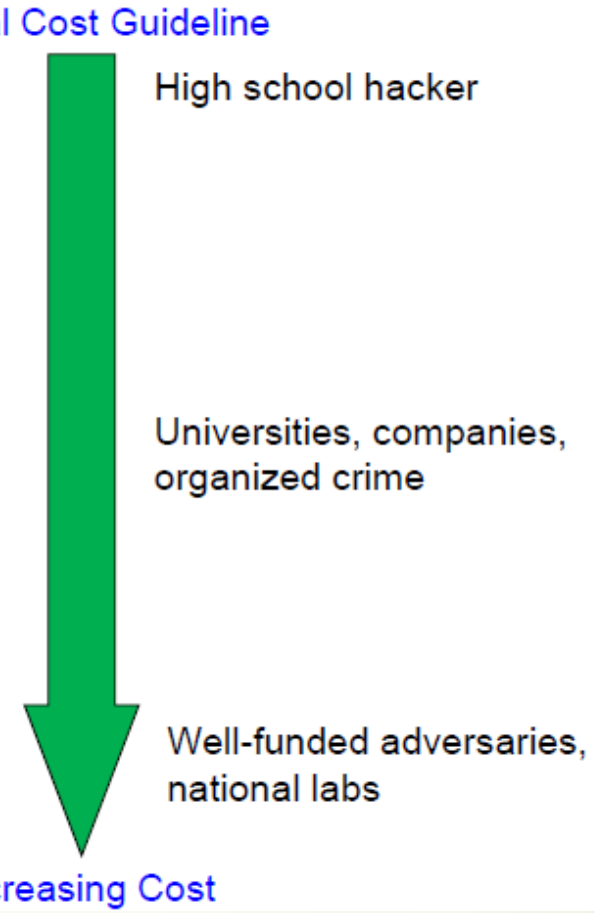
Load/Validate Phase-0 Code



Source : Advanced Design Security by G. Richard Newell, Security Forum, 2012

Hierarchy of Technical Attacks

- Protocol
  - Eavesdropping
  - Man-in-the-middle
  - Replay
  - Relay
  - Other protocol design attacks
- Side-Channel (noninvasive, passive)
  - Timing
  - Simple power analysis (SPA)
  - Differential power analysis (DPA)
  - Electromagnetic emanations (xEMA)
- Active (non-invasive)
  - Fault injection (laser or power glitch)
  - Temperature (cold SRAM effect)
  - Clock manipulation
- Semi-invasive and invasive
  - Optical
  - Electron microscope
  - Focused ion beam (FIB)
- Cryptographic



Source : Advanced Design Security by G. Richard Newell, Security Forum, 2012