

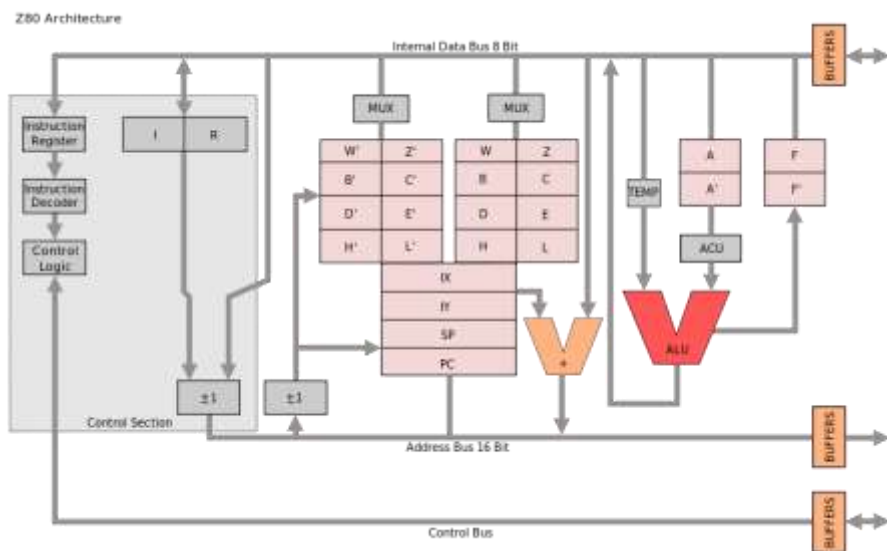


# Customizable System-on-Chips (cSoCs): *The New Platform for Custom Security Applications*

Richard Newell  
for the HIS Initiative Annual Meeting  
November 16, 2011

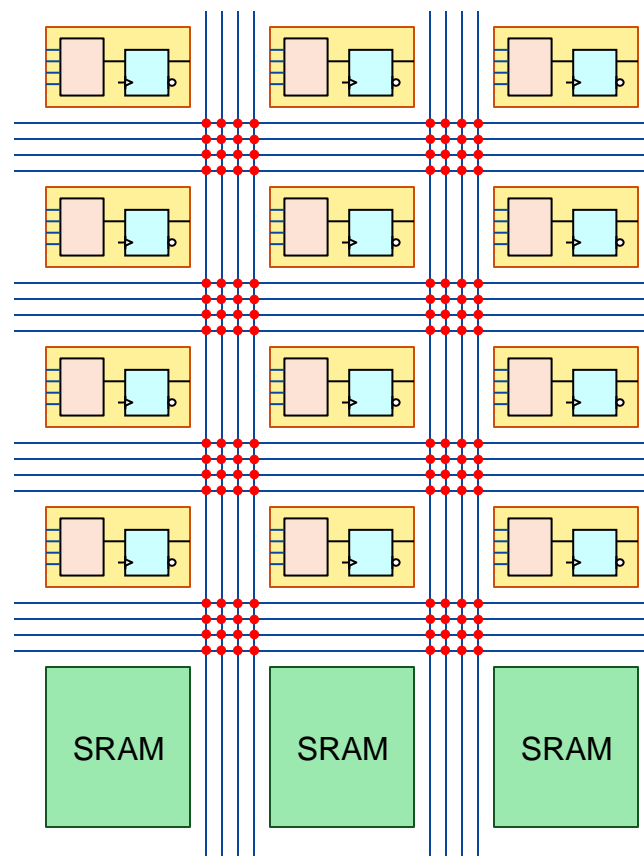
# What is a “cSOC”?

- Customizable System-on-Chip = cSoC = MCU + FPGA



Primarily Sequential  
• Shared Resources

+



Primarily Parallel  
• Fine Grained

# Some things just go well together...



80's Reese's Peanut Butter Cups commercial

# Advantages of Each Technology

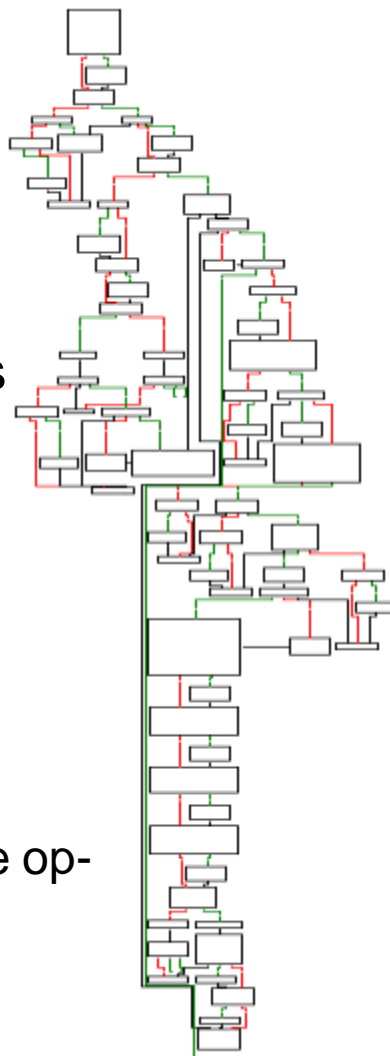
## CPU Architecture

### ■ Good:

- Good at complex algorithms
- Efficient reuse of hardware resources

### ■ Poor

- Low parallelism
- Hard to scale
- Power hungry
  - Many sub-sections working to do simple op-code execution



## FPGA Architecture

### ■ Good

- Fine-grained resources
- High Parallelism possible
- Flexible scheduling options
- Easy to pipeline

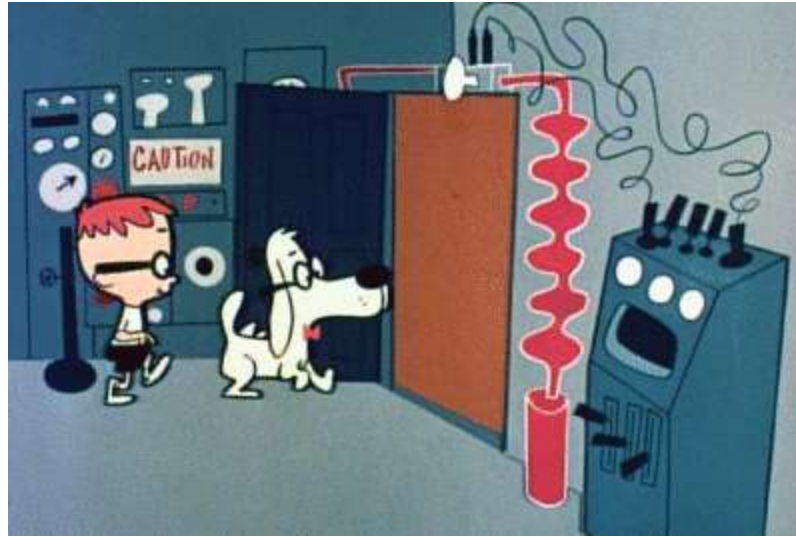
### ■ Poor

- Not good at complex algorithms with a lot of branching
  - Must resort to CPU-like implementation
- Programmable gates use more transistors than fixed gates

# Progress Towards the cSoC

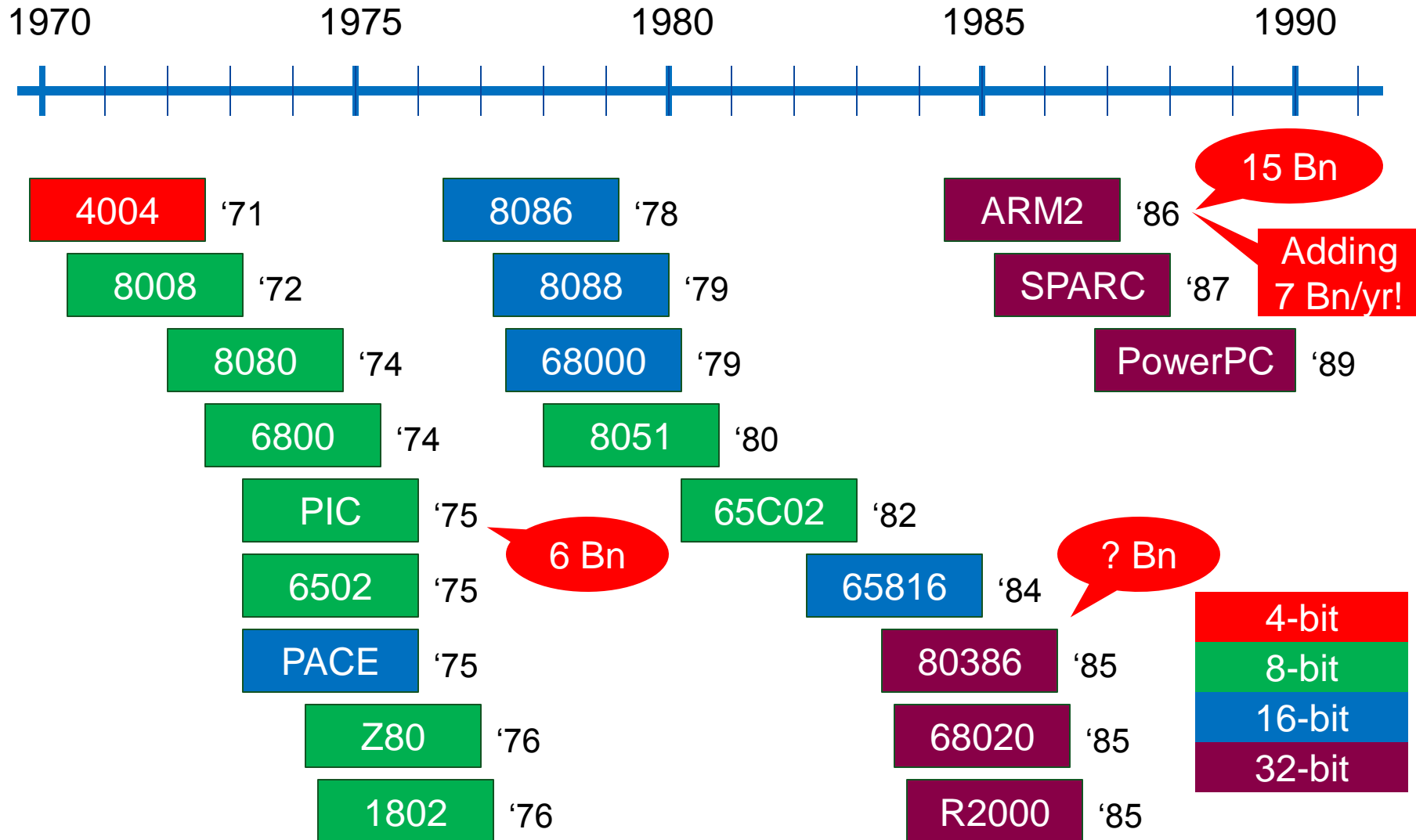


# Historical Trends Leading to the cSoC

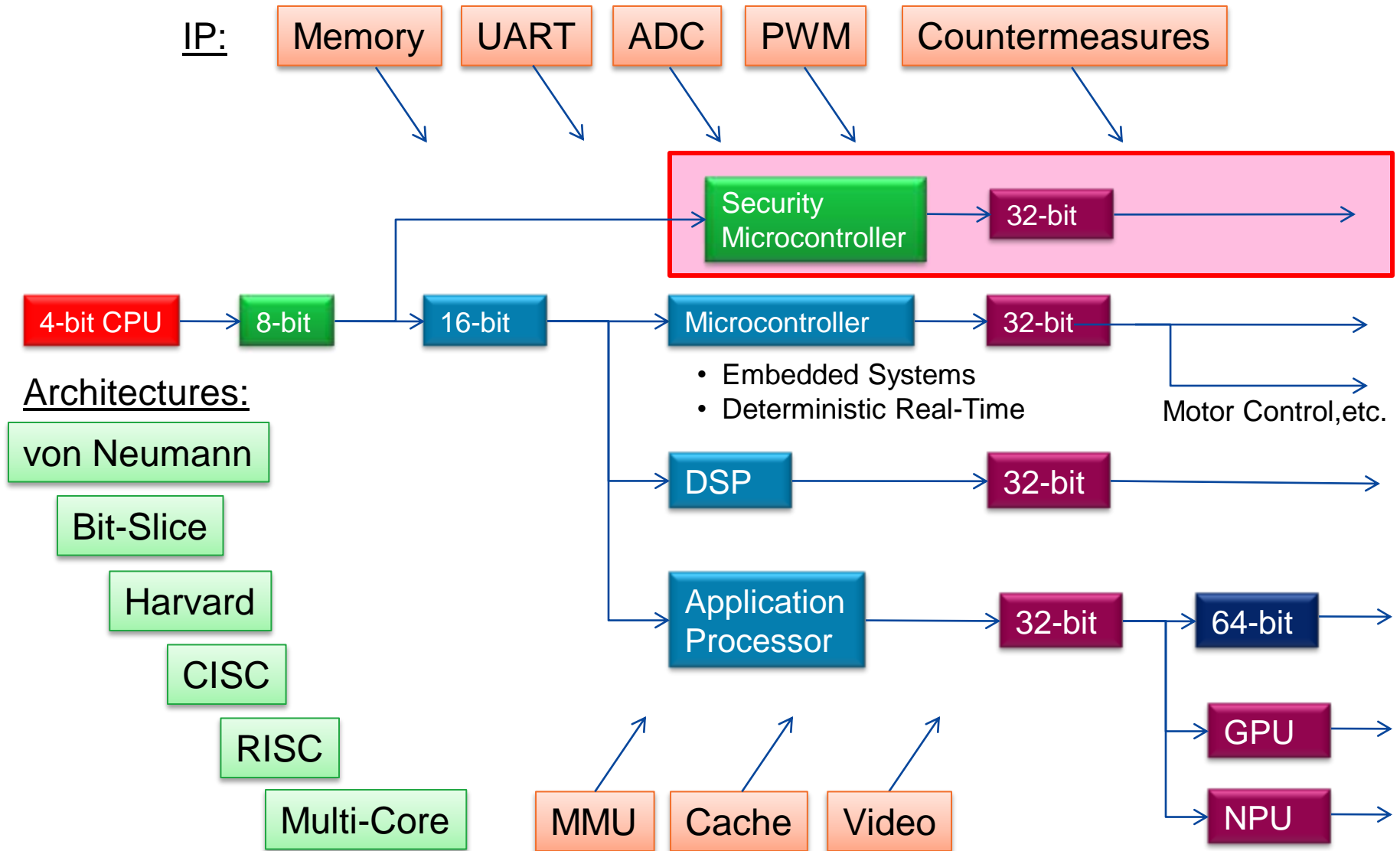


- “Sherman, set the WABAC machine for exactly 40 years and 1 day ago, to November 15, 1971.”
- “Done, Mr. Peabody. Let’s see what happened that day!”
  - Intel released the 4004 to the public
    - The first publicly available complete general-purpose CPU on an integrated circuit

# Microprocessor Early Development History



# Microprocessor Progress and Diversification



# Early Security-Microcontroller Applications



Telephone Cards



Transportation Cards



Credit & ATM Cards

Mobile Subscriber ID

Anti-Counterfeiting



Conditional Access



## Main Applications:

- Stored Value
- Authentication
- Cost Sensitive

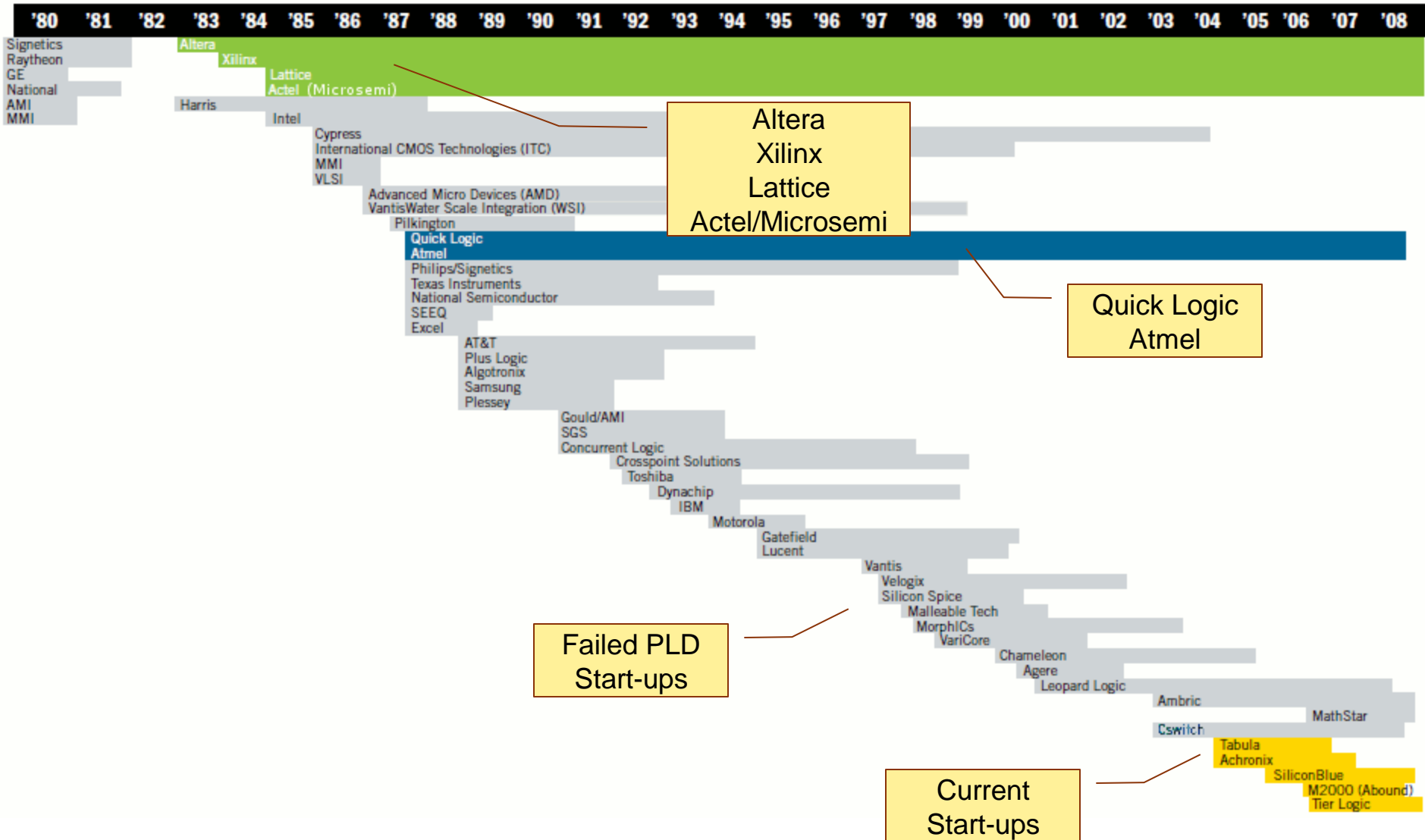
## Interfaces:

- Simple Serial

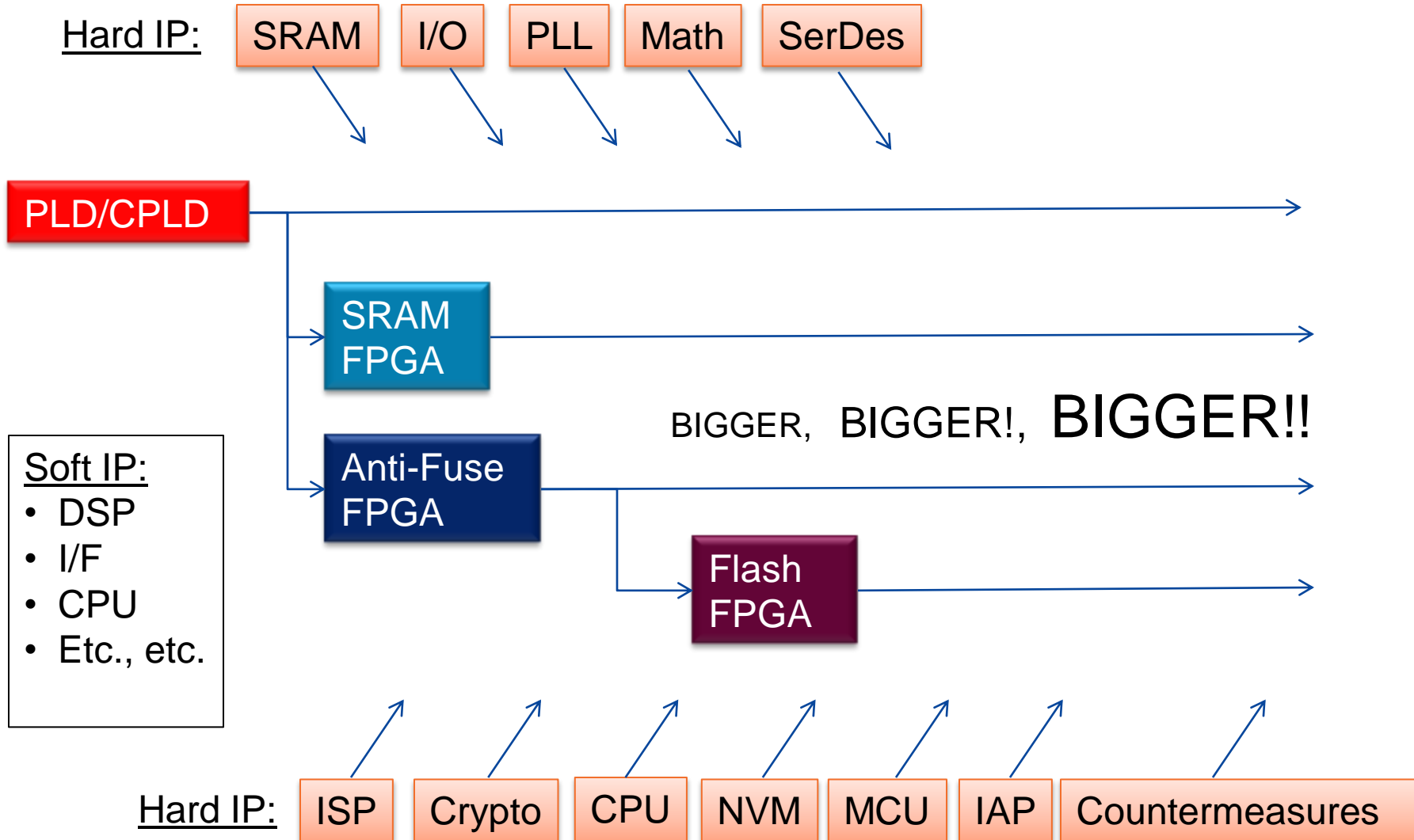
## Architecture:

- 8-bit Harvard
- Metal-mask ROM

# History of PLD Start-ups



# FPGA Progress



# FPGA Capacity

1985

2011

64-128 Logic Elements  
(LUT + FF)

500,000+ Logic Elements  
(LUT + FF)

1-2 $\mu$ m fabrication technology

0.028 $\mu$ m fabrication technology

4 Orders-of-Magnitude  
growth due to Moore's Law



# One Security Customer's Use of FPGAs



Secure Telephone

Packet Encryption



Imaging System

Helicopter



Encrypted  
USB  
Flash Disk



Secure Telephone



Secure Cell Phone

Frequency-Hopping Military Radio



Secure IP Encryption

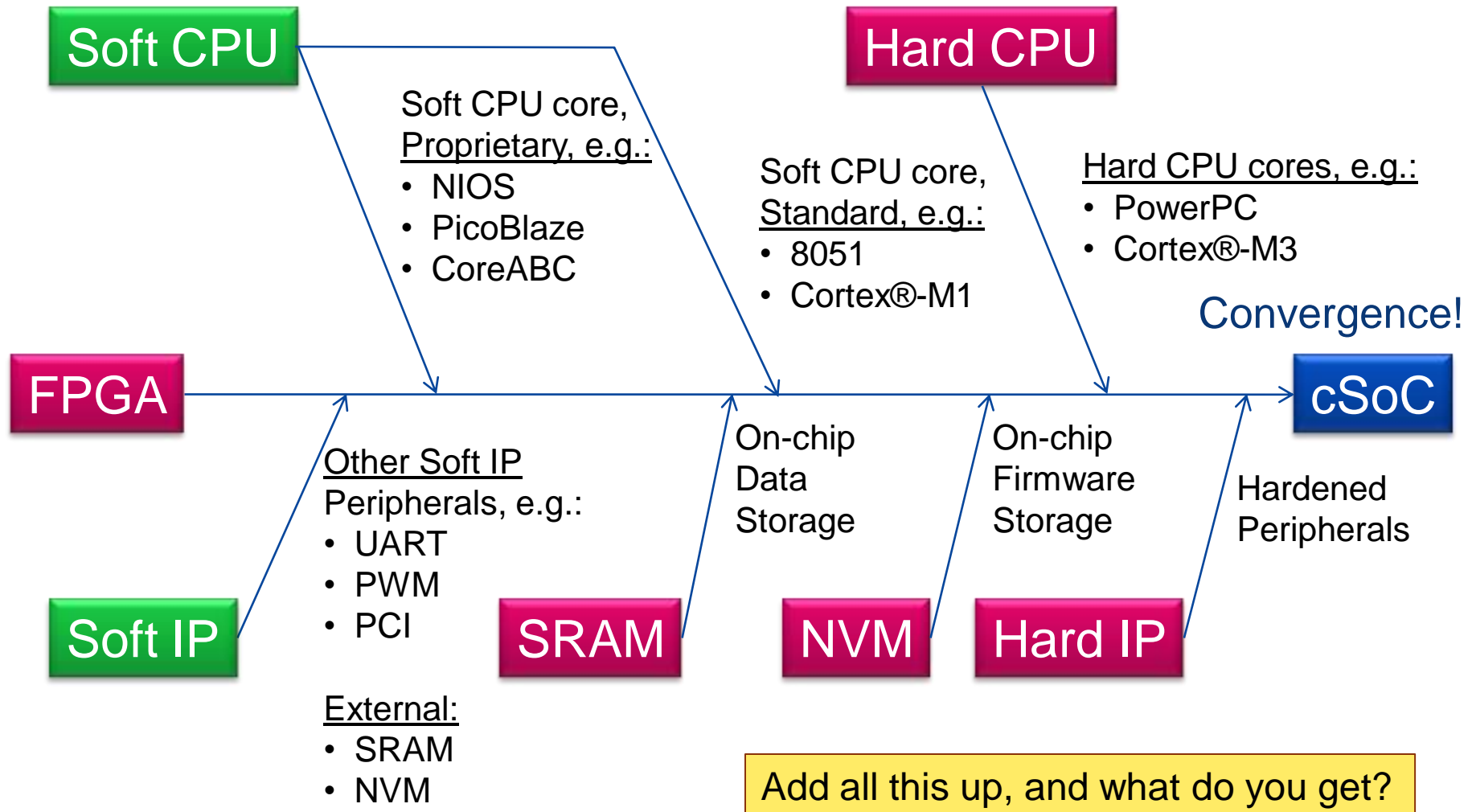


Military Hand-held Radios

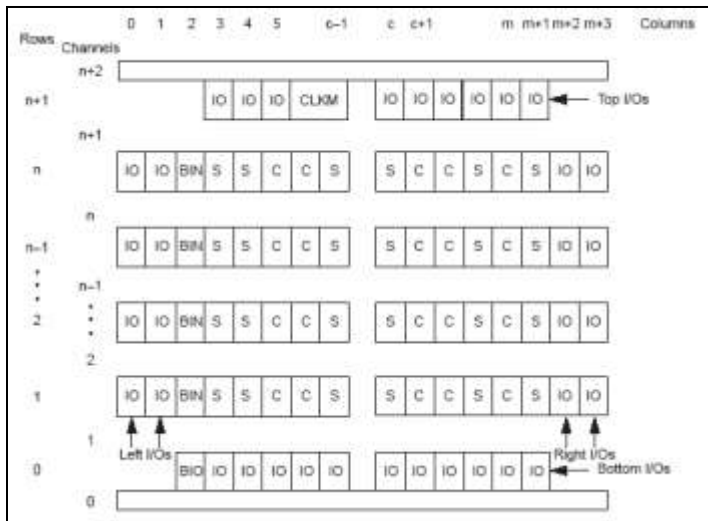


Night Vision

# FPGA's Long Engagement with CPUs



# Not Your Father's FPGA!

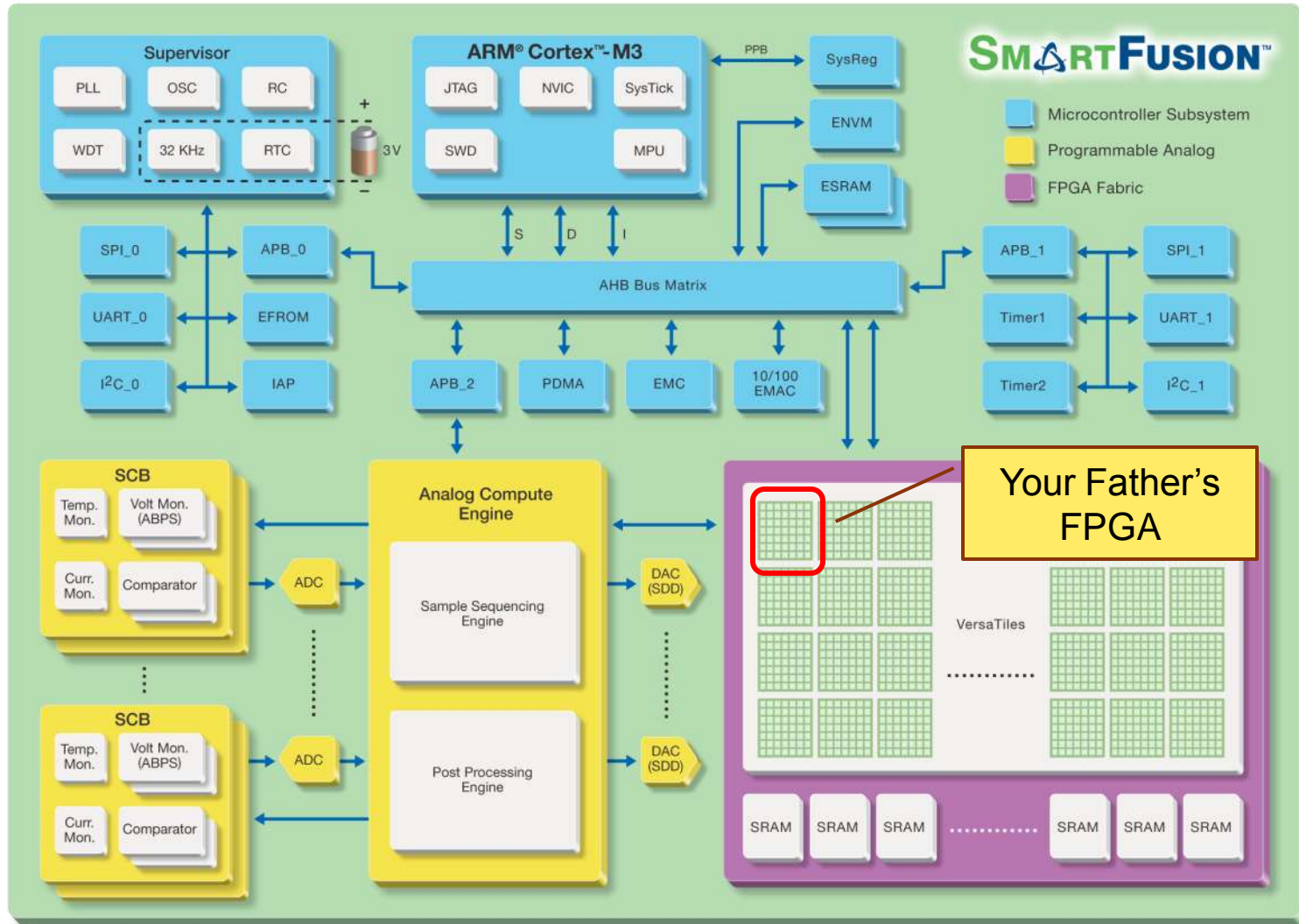


ACT 3 Generalized Floor Plan



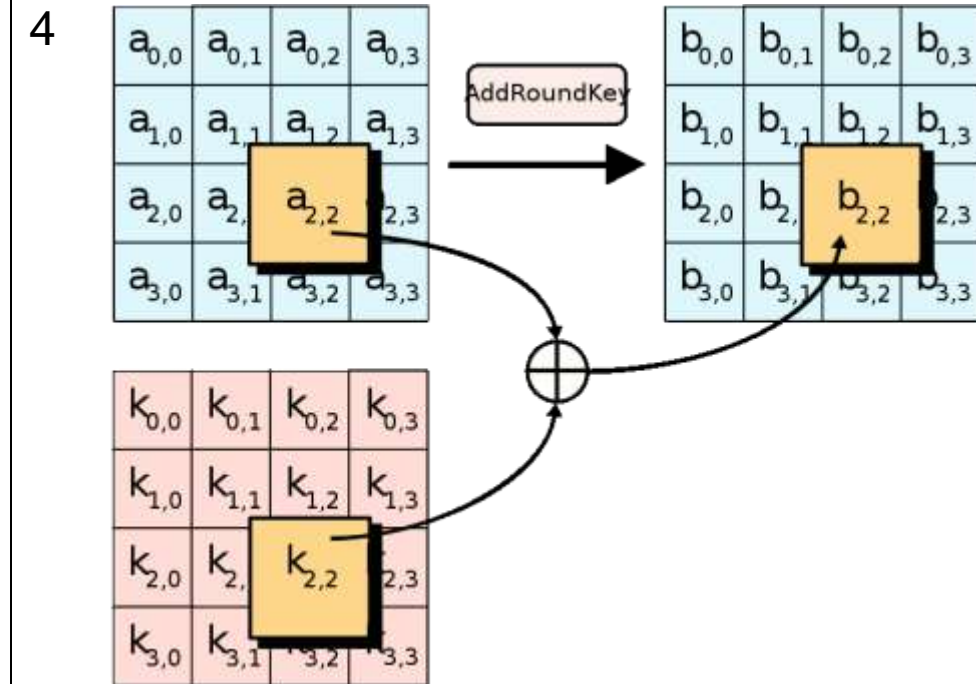
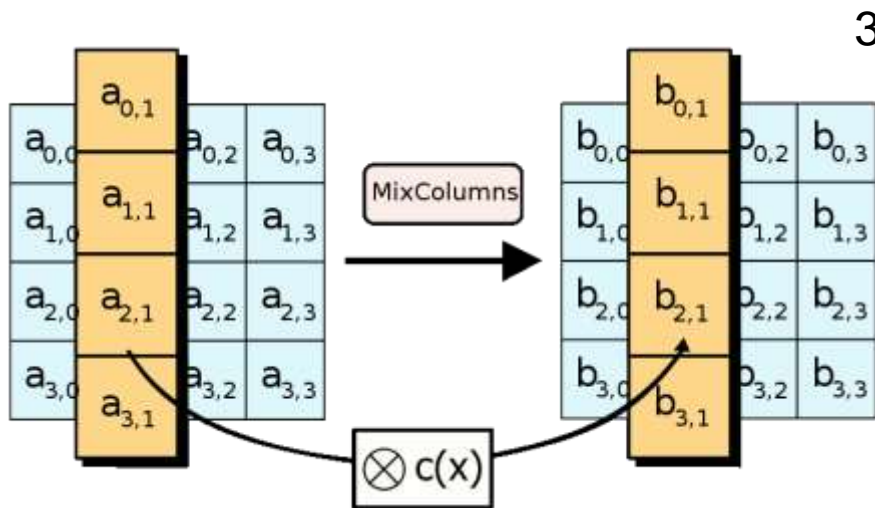
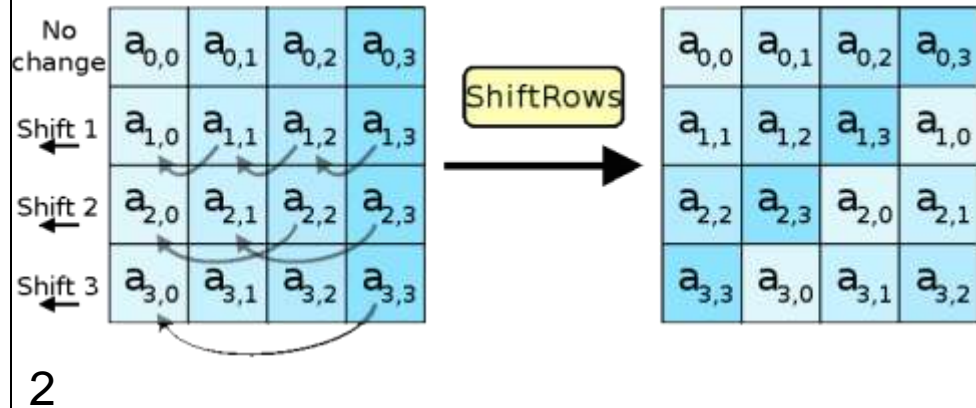
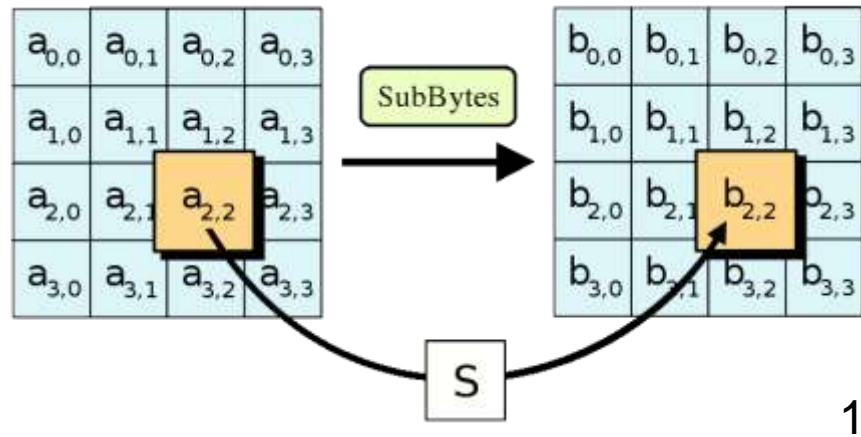
My mentor, Harold Morris, showing off the latest op-amp technology way back when

# State-of-the-Art cSoC: SmartFusion™



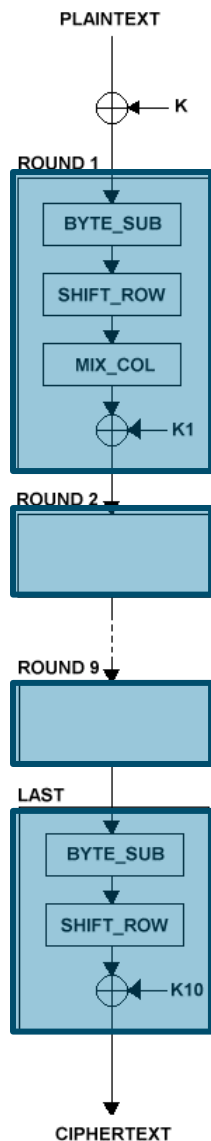
# Example of FPGA Parallelism Scheduling Options

# Advanced Encryption Standard (AES)



Repeat "1" thru "4" 10 to 14 times  
(depending upon key size)

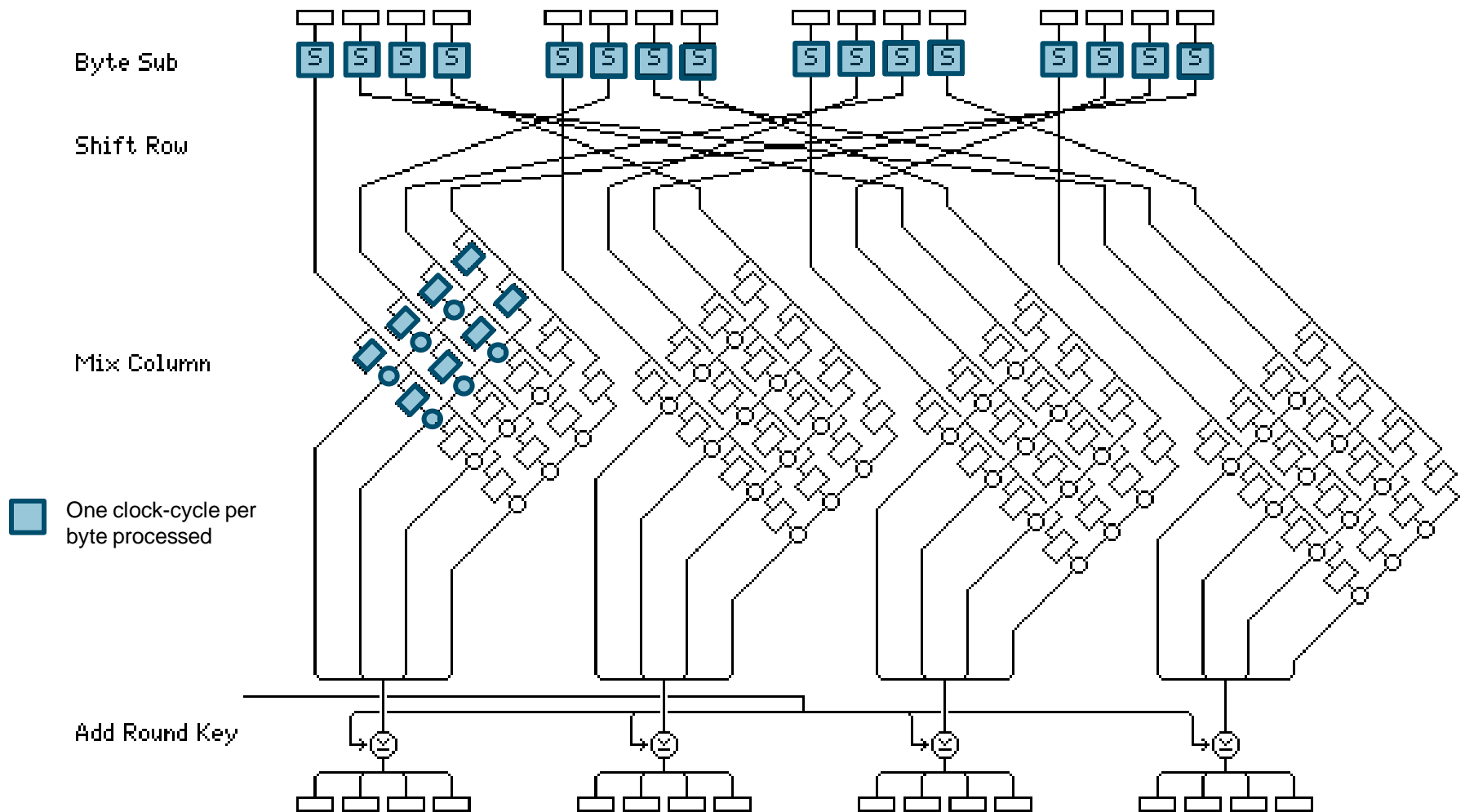
# AES



- AES-128: 10 Rounds
- AES-256: 14 Rounds
- AES is designed using 8-bit primitive operations

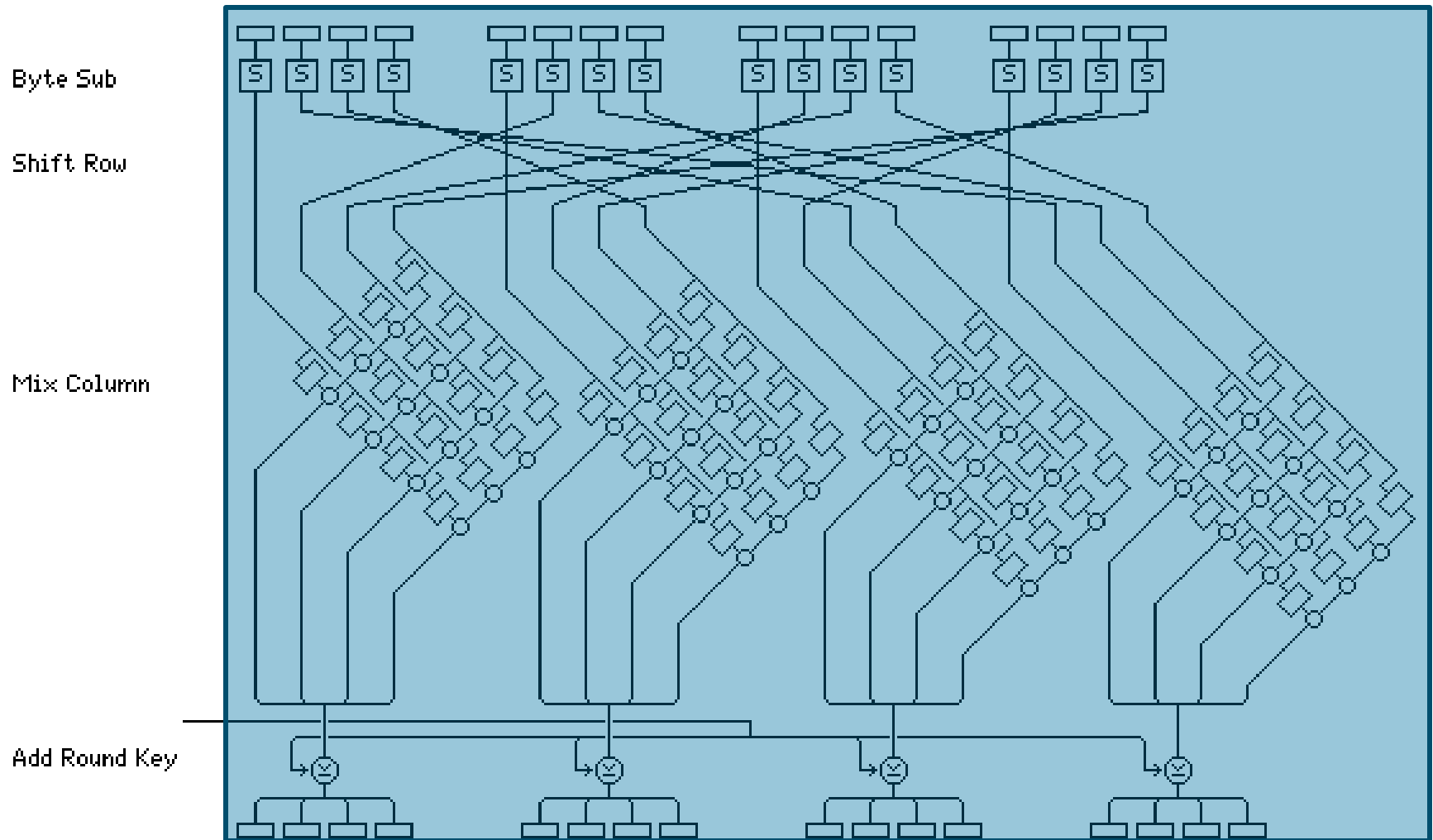
# Advanced Encryption Standard: 8-bit $\mu$ P

- Uses a few hundred clock cycles per round



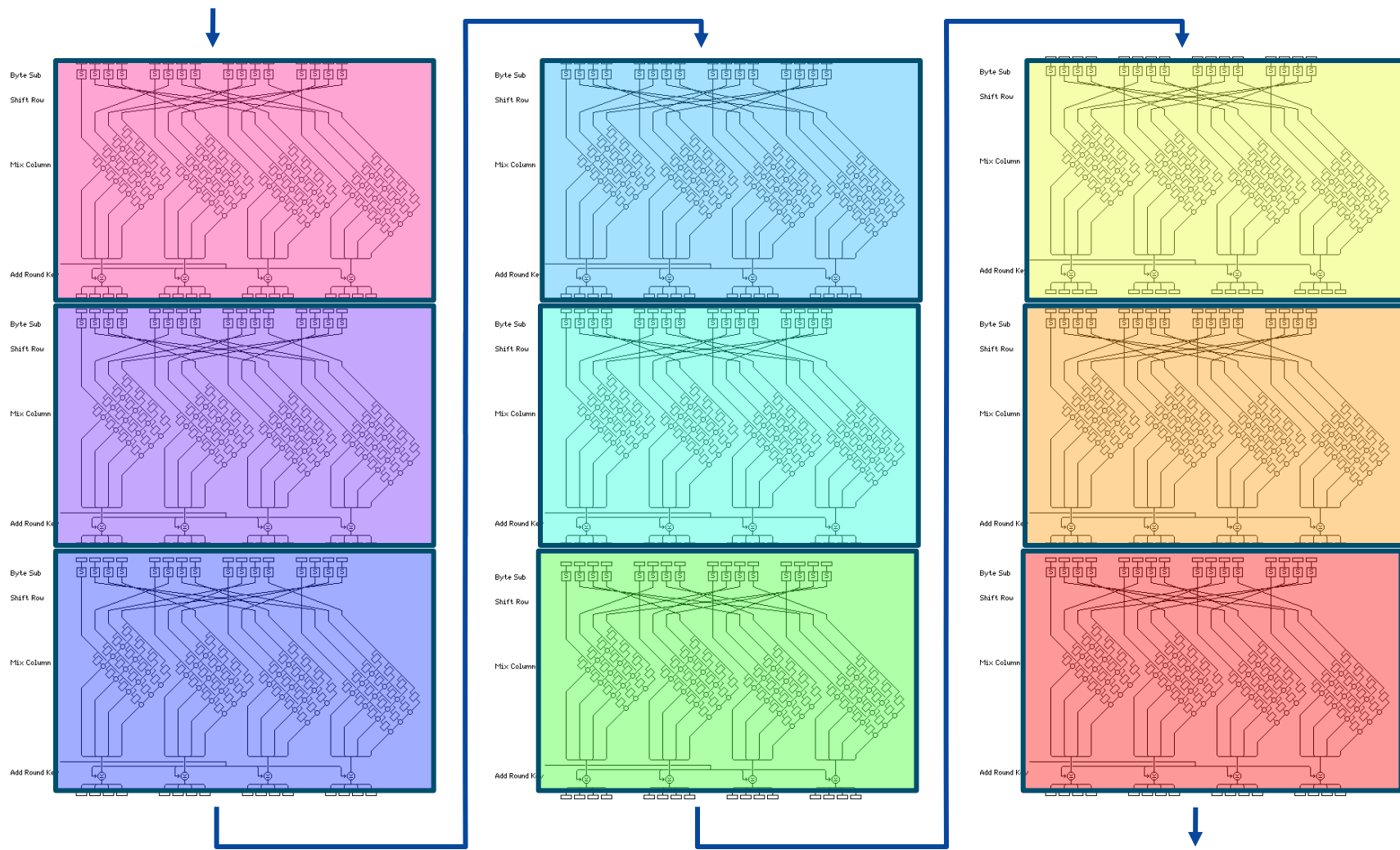
# Advanced Encryption Standard: 16 S-box FPGA

- Uses one clock cycle per round



# Advanced Encryption Standard: unrolled FPGA

- Does all rounds in parallel for a throughput of one full encryption per clock



# Performance Comparison: HW vs. SW

## Firmware only

- With DPA and fault countermeasures
- Performance-optimized for Cortex®-M3

(100 MHz, 32-bit  $\mu$ C)

- RSA 1024 ~ 200 ms
- AES 256 ~ 650  $\mu$ s (0.2 Mbps)
- ECC 256 ~ 80 ms

## FPGA

- AES 128
  - 21 Mbps – 1440 Mbps  
100 to 7000 times faster
- ECC 256
  - ~ 670  $\mu$ sec per signature on a low cost FPGA using the Vehicle-Area Network (VANET) engine\*  
120 times faster
- See last May's keynote by Christof Paar

# Security Considerations

# Definitions: Design Security vs. Data Security

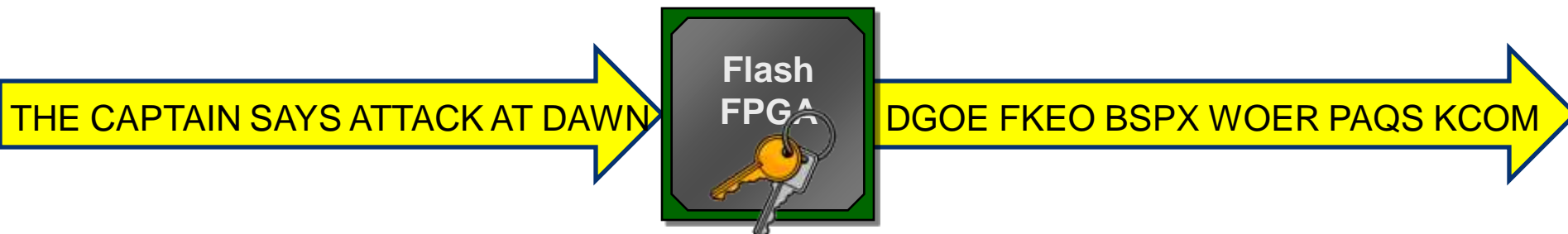
## ■ FPGA Design/Device Security

- Making sure that the *FPGA Design* is protected and the IP owner's security intent is respected

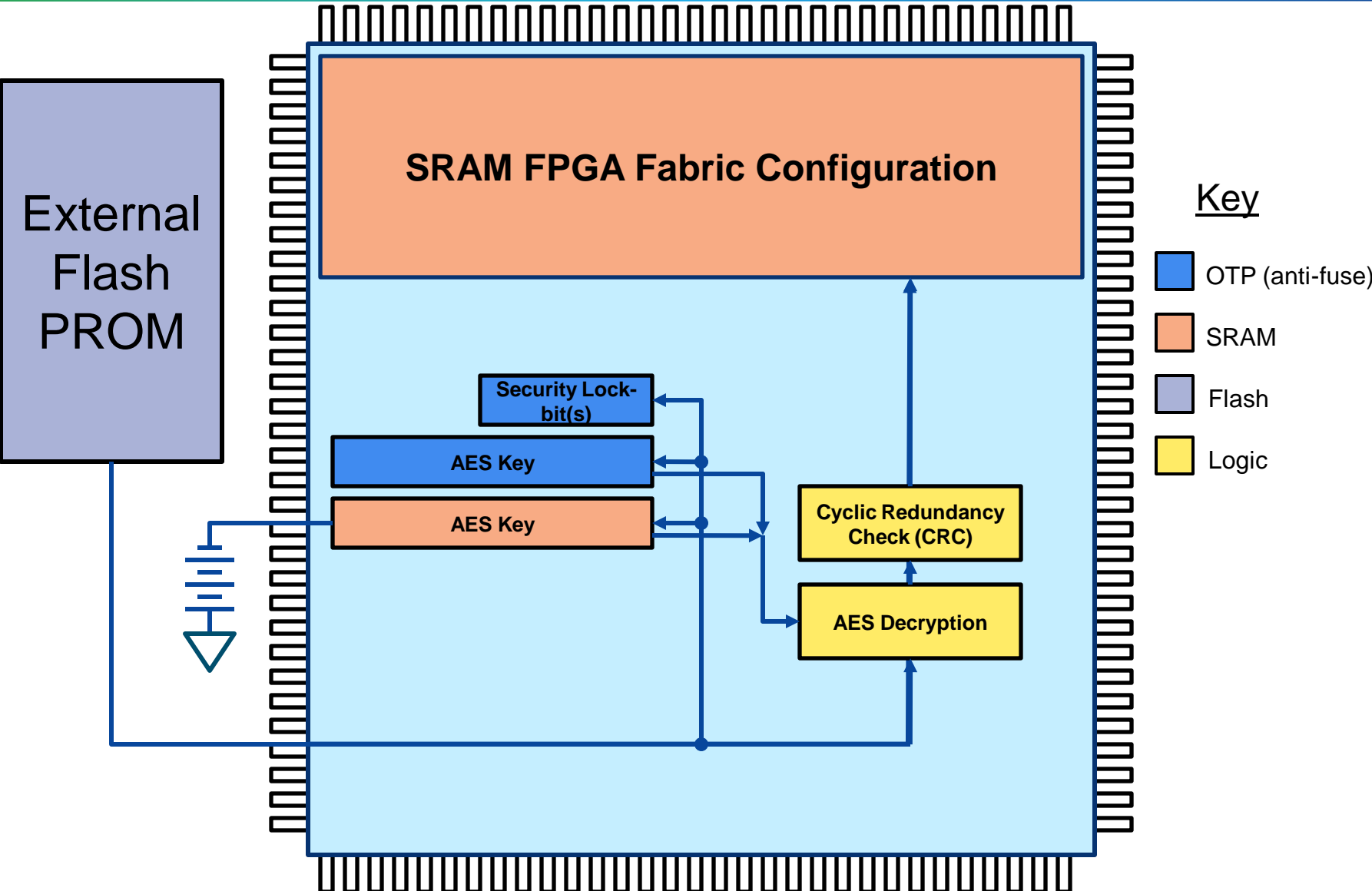


## ■ Data Security

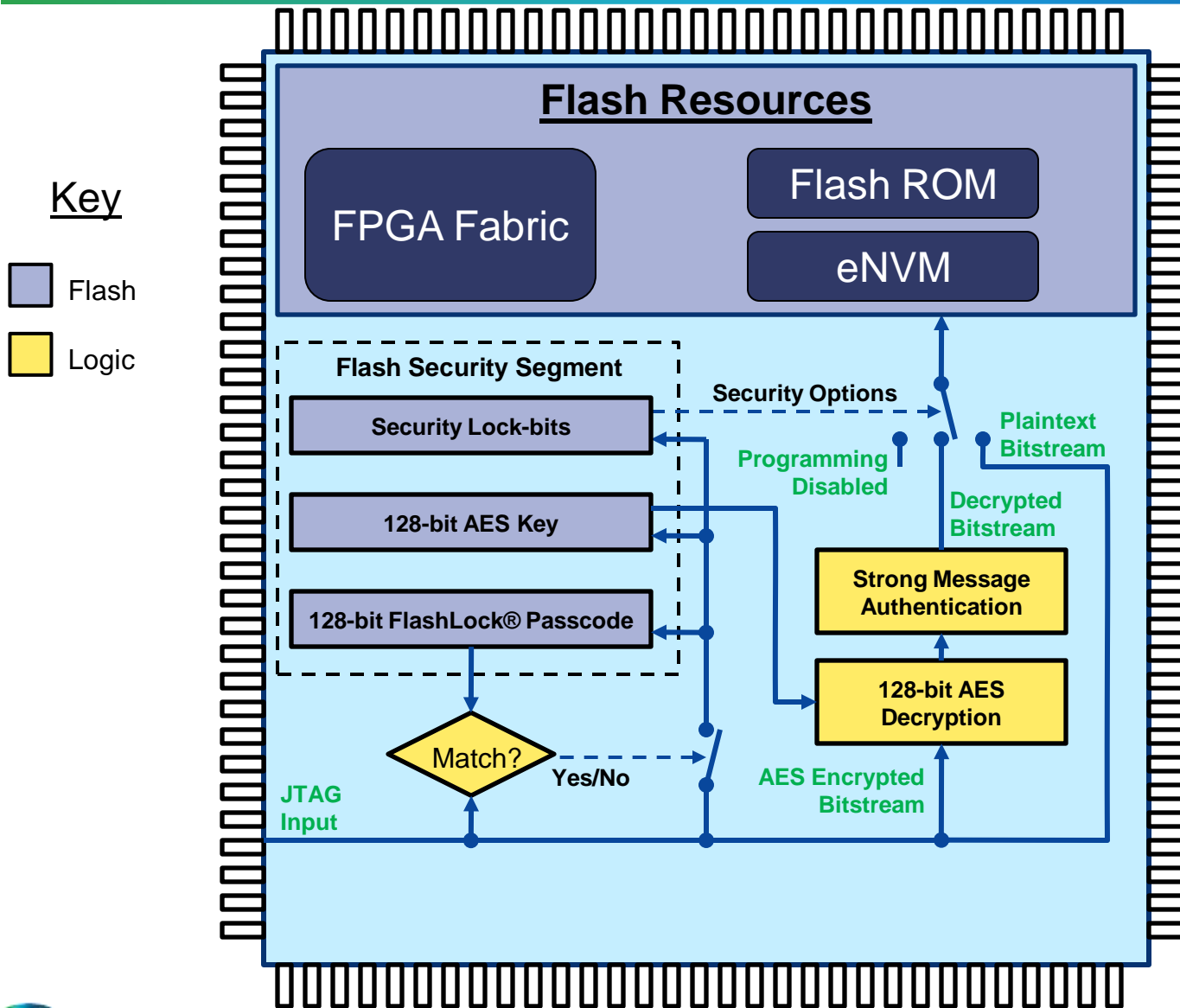
- The *Application* programmed into the device meets its security objectives (authenticity, confidentiality, integrity, etc.)



# Typical SRAM FPGA Hardware Security Architecture



# Typical Flash FPGA Hardware Security Architecture



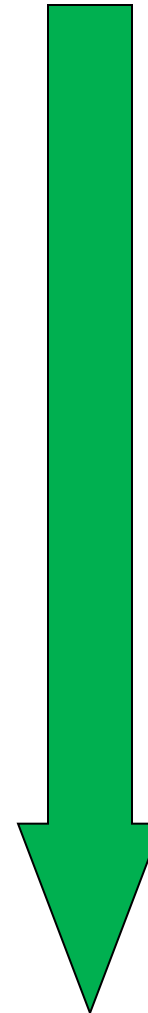
ProASIC®/B



# Hierarchy of Technical Attacks

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

## General Cost Guideline



High School Hacker

Universities, companies,  
organized crime

Well-funded adversaries,  
national labs

Increasing Cost

# Security Boundary

- In general, there are two ways to secure a device:
  - Put it in a secure location, such as a limited-access computer server room, and secure the communications interfaces that leave the room
  - If the unit is exposed to malicious physical attacks, then the device will have to be tamper-resistant, and protect itself



Secure  
Data Center



PCI Card  
Multi-chip security module

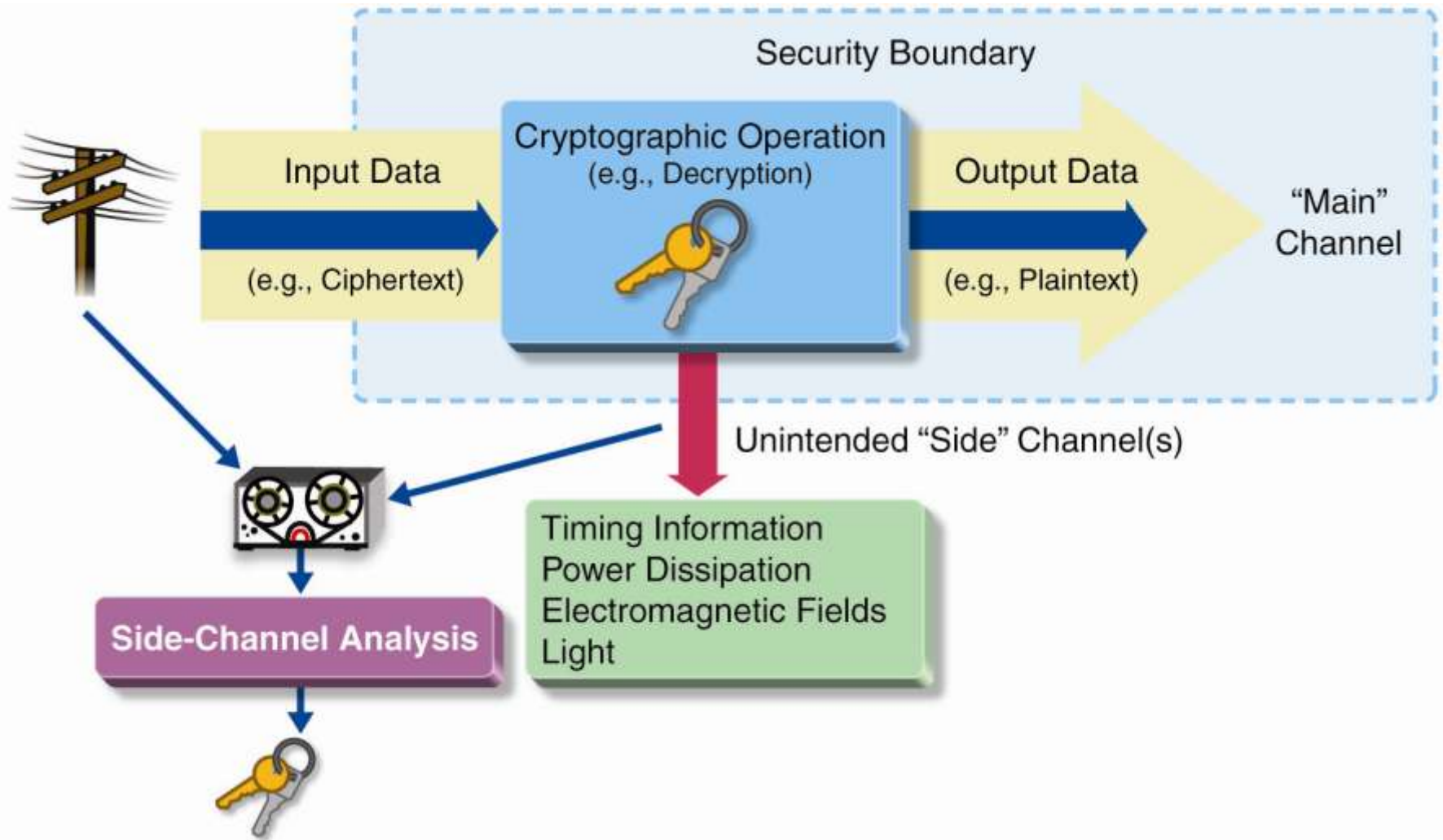


Smart Card  
Single-chip security module



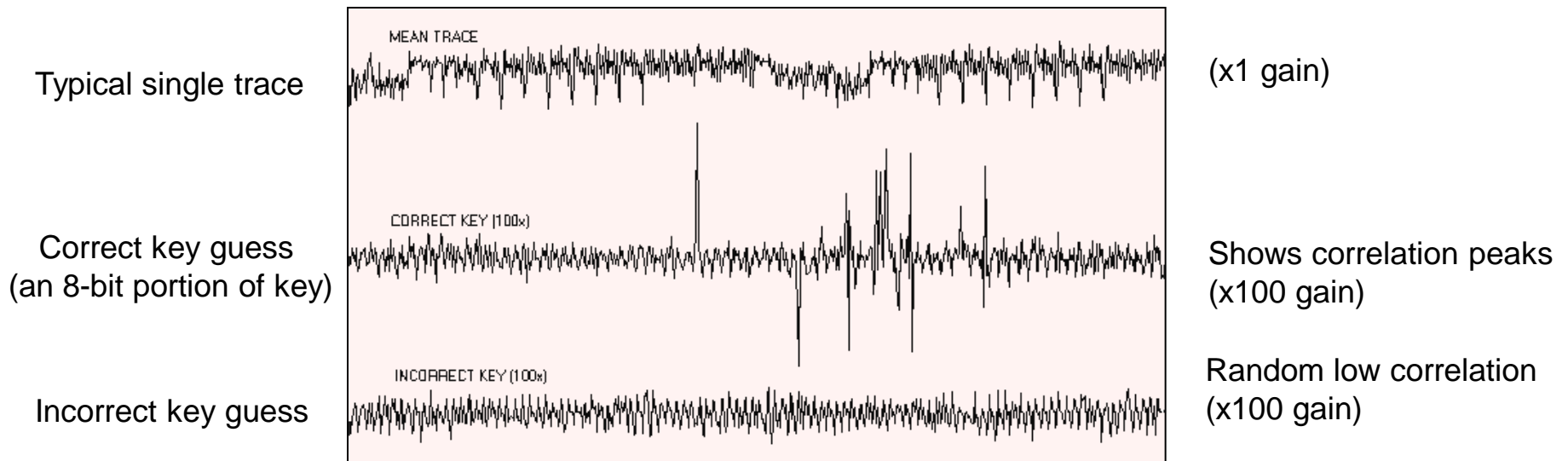
Flash FPGAs can be used as a single-chip security module, or part of a larger system

# Side-Channel Analysis



# Differential Power Analysis (DPA)

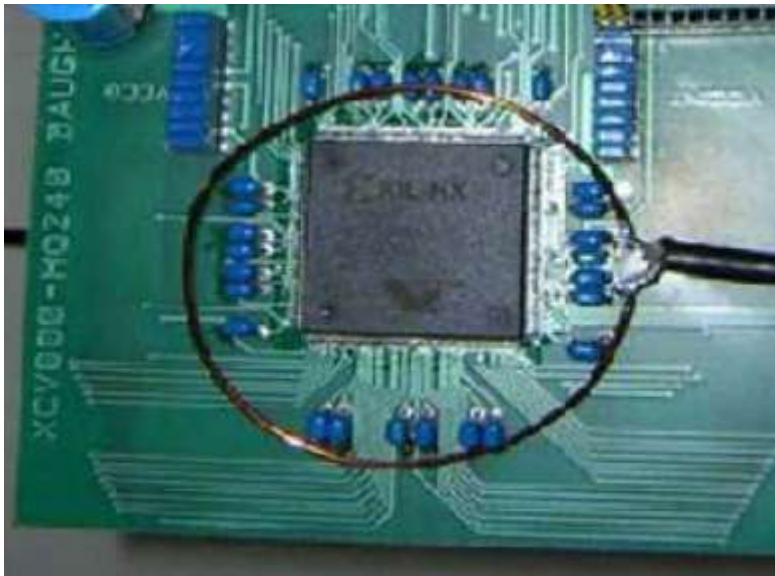
- Observe a series of cryptographic transactions
- Apply statistical tests to correlations in computational intermediates
- Results recover the key and other secrets
- First published in 1999 by Paul Kocher and his associates at Cryptography Research, Inc.
  - Major impact on development of the SmartCards used in banking, set-top boxes, etc.



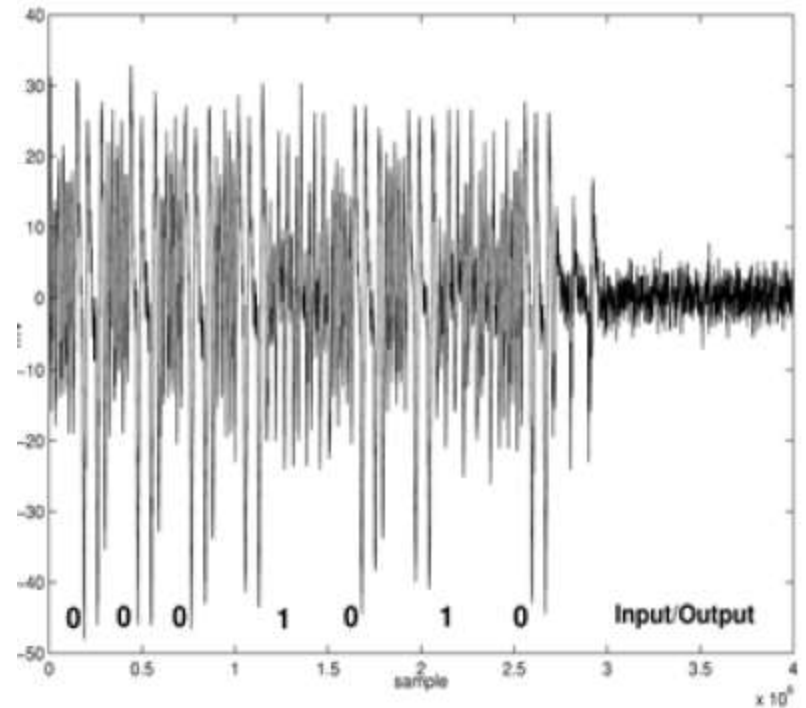
[Paul Kocher et al, Proc. CRYPTO 1999]

# Simple Electro-Magnetic Analysis (SEMA)

FPGA and antenna



EM Trace  
Insecure ECC implementation

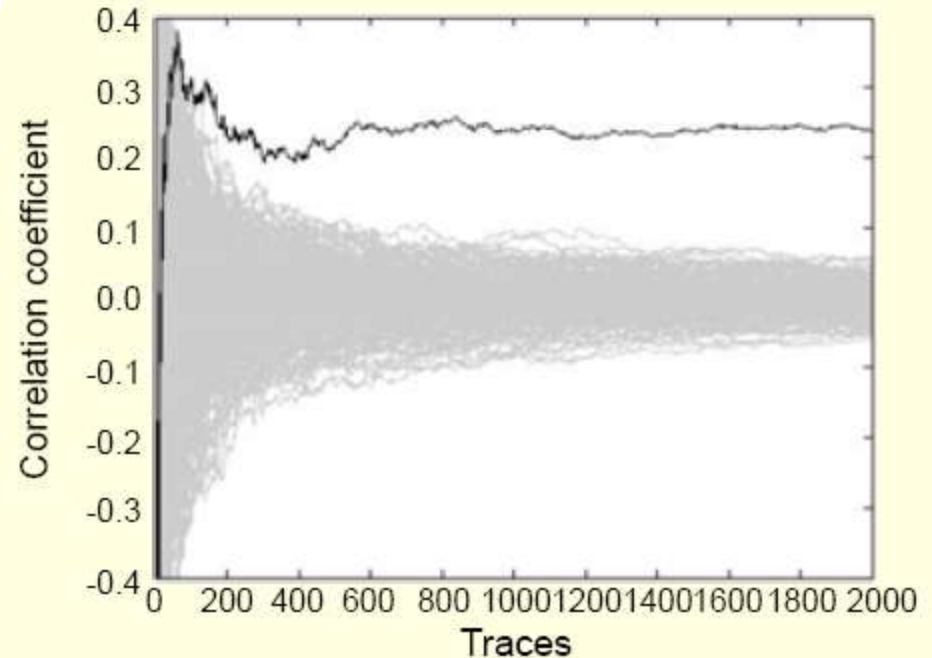
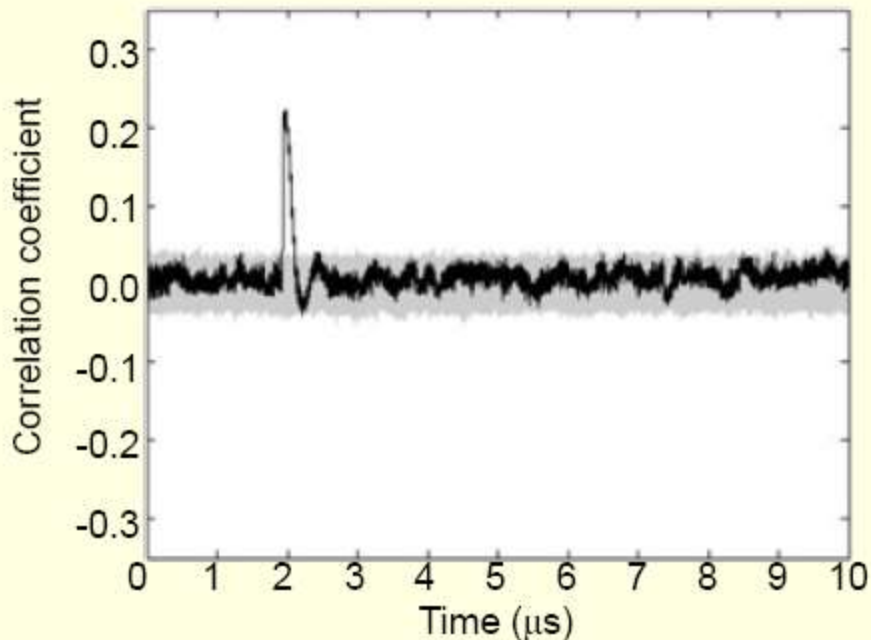


[E. Demulder EUROCON 2005]

ECC = Elliptic Curve Cryptography

# DPA of a cipher implemented in an FPGA

1 correct key guess shown with **black** trace (an 8-bit portion of key guessed)  
255 incorrect key guesses shown with **gray** traces



Correlation estimate time trace for correct key guess shows correlation peak well differentiated from traces for 255 incorrect key guesses (2000 measurements with random ciphertext used for correlation estimates)

Correlation estimates improve with the number of measurements used.

Correct key guess stands out from the 255 incorrect key guesses when 200 traces (or more) are used

[ChangKyun Kim, Martin Schl affer, and SangJae Moon,  
ETRI Journal, April 2008]

# DPA Attack on SRAM FPGA Design Security

## On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks

– Extracting Keys from Xilinx Virtex-II FPGAs –

Amir Moradi  
Horst Görtz Institute  
for IT-Security  
Ruhr-University Bochum,  
Germany  
amir.moradi@rub.de

Alessandro Barenghi  
Dipartimento di  
Elettronica e Informazione  
Politecnico di Milano, Italy  
barenghi@elet.polimi.it

Timo Kasper  
Horst Görtz Institute  
for IT-Security  
Ruhr-University Bochum,  
Germany  
timo.kasper@rub.de

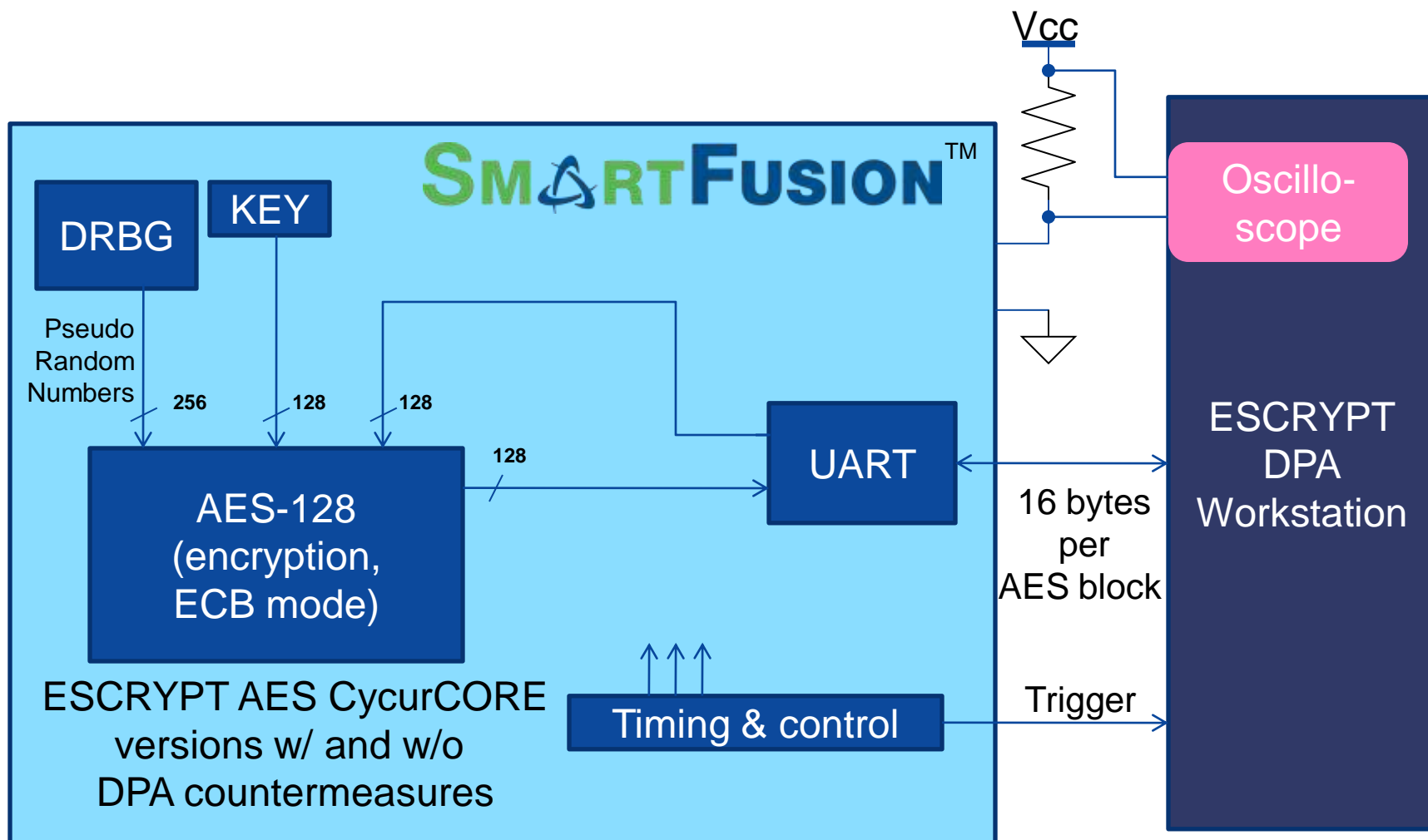
Christof Paar  
Horst Görtz Institute  
for IT-Security  
Ruhr-University Bochum,  
Germany  
christof.paar@rub.de

## On the Portability of Side-Channel Attacks

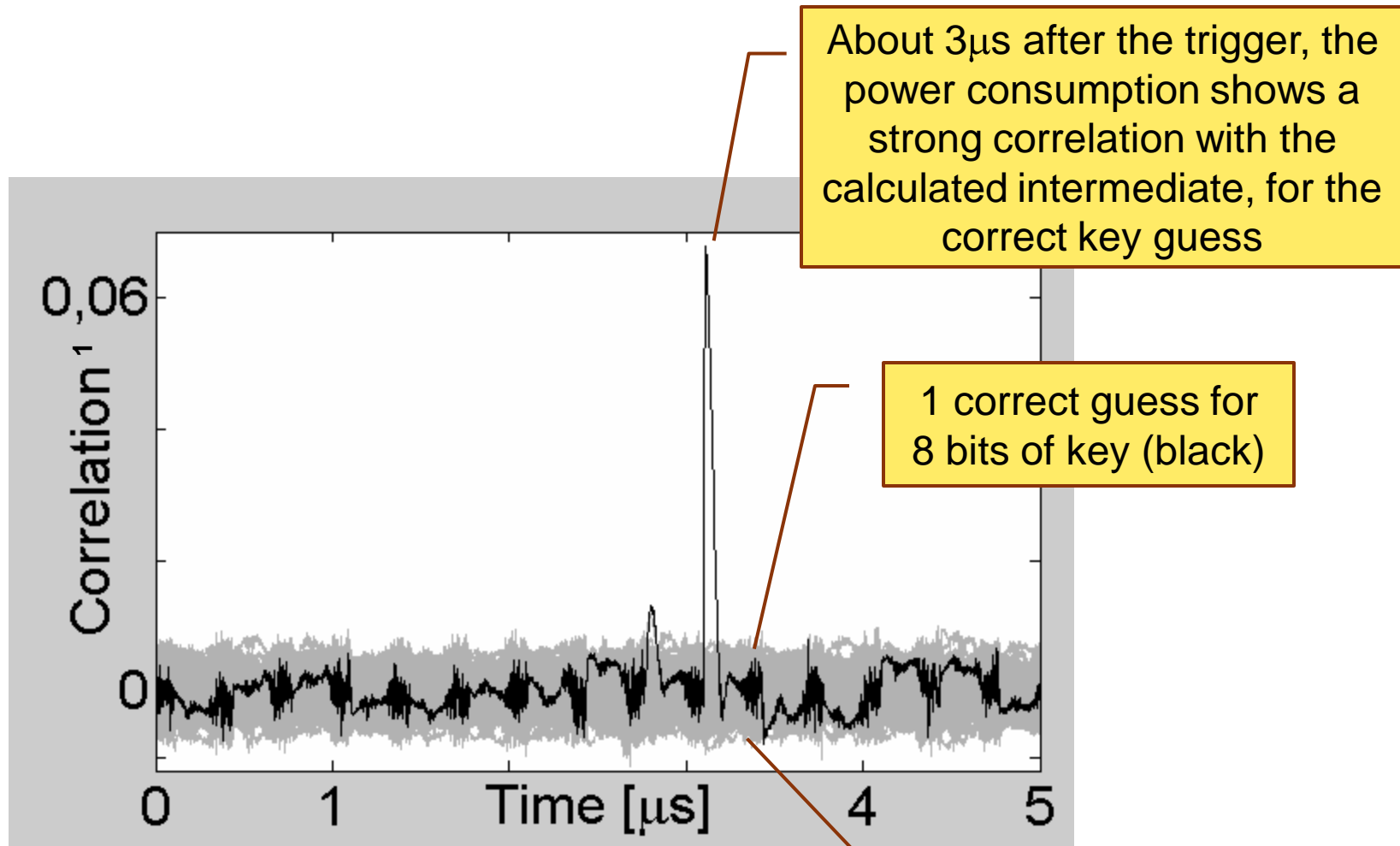
– An Analysis of the Xilinx Virtex 4 and Virtex 5 Bitstream Encryption Mechanism –

Amir Moradi, Markus Kasper, Christof Paar

# Test Set-up Block Diagram

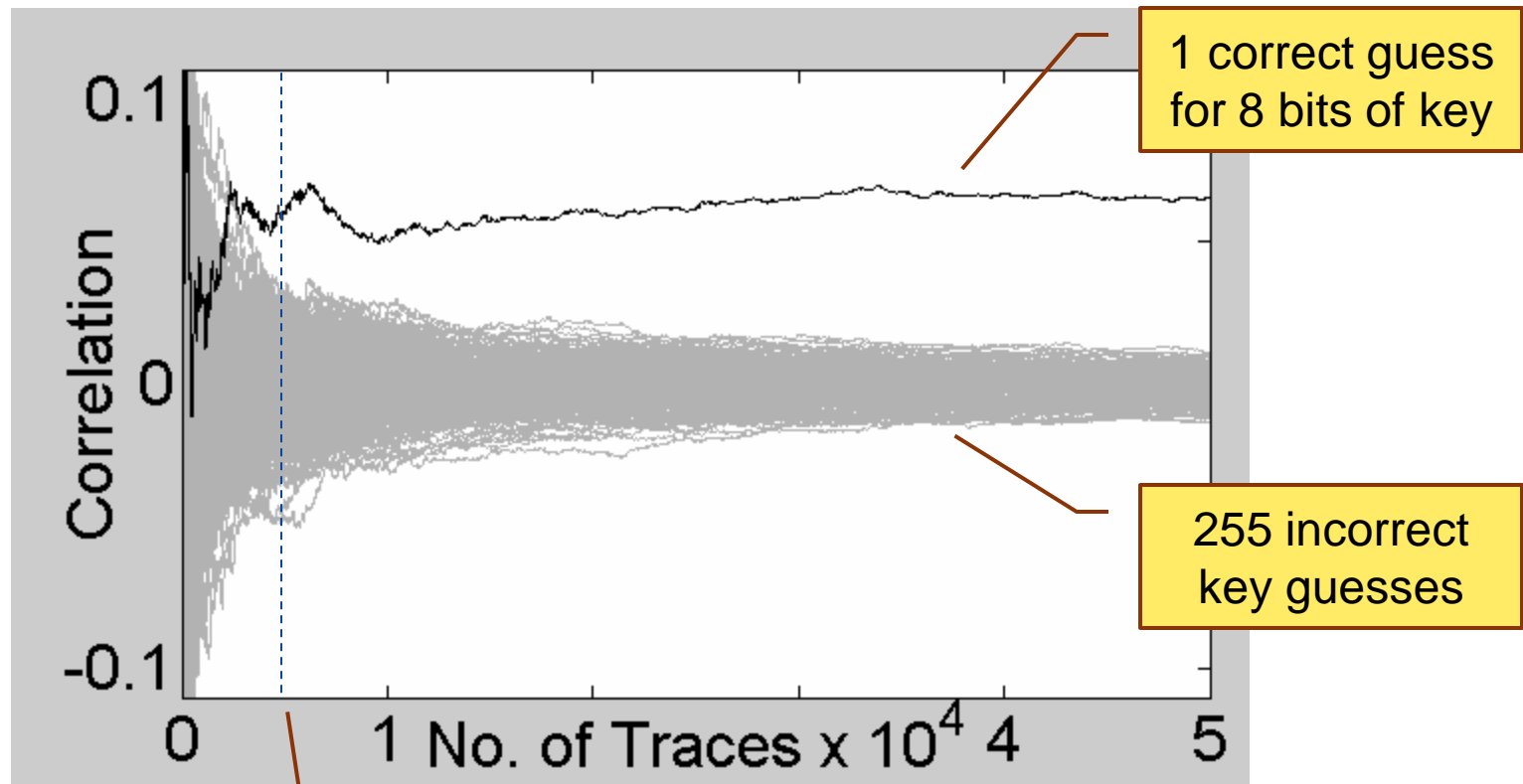


# Correlation Power Trace for 256 key guesses Without Countermeasures



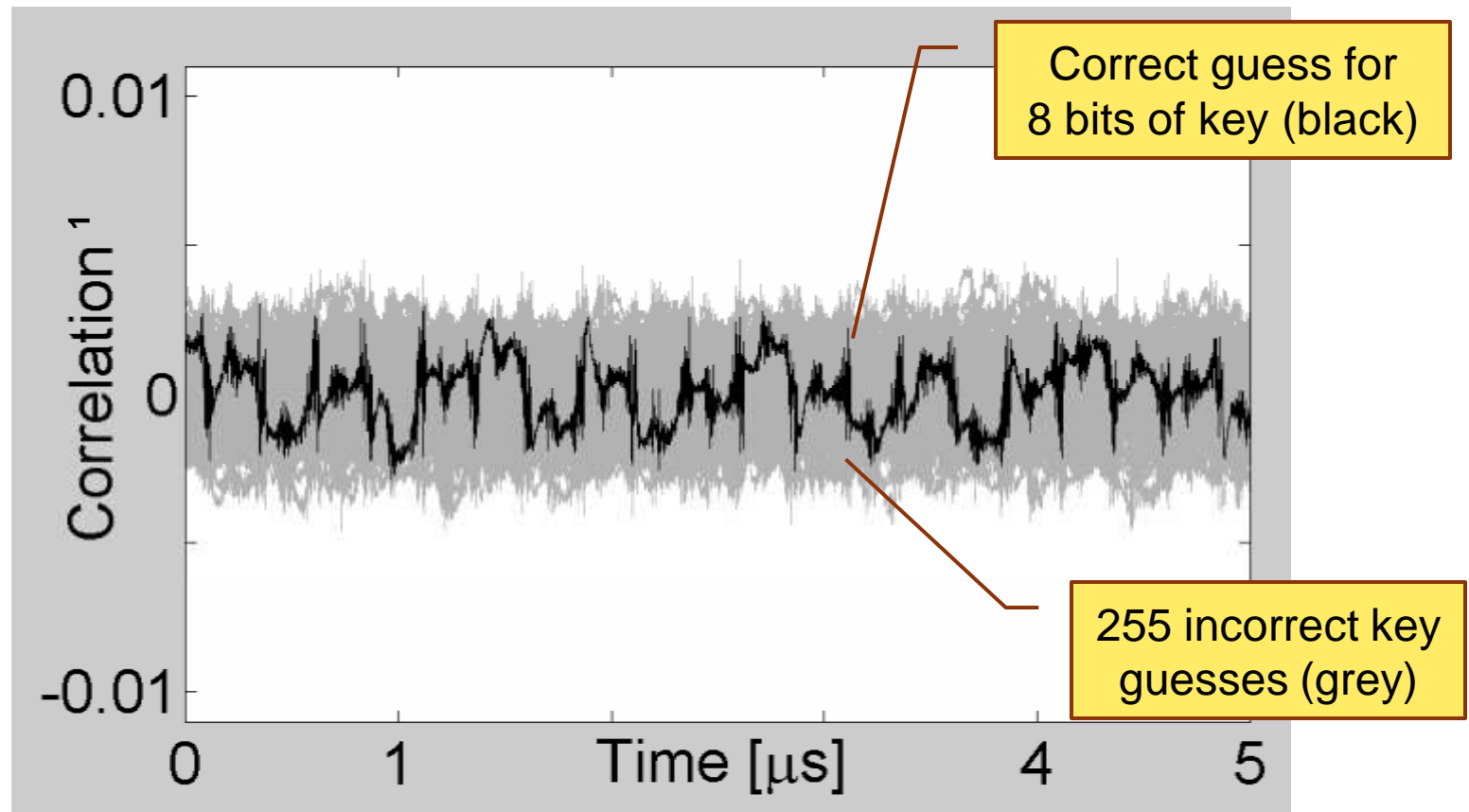
<sup>1</sup> Correlation vs. time estimated from 200,000 power measurements

# Correlation vs. Number of Measurements Without Countermeasures



After approx. 5000 measurement traces the correct key shows a consistently higher correlation estimate than any other key guess

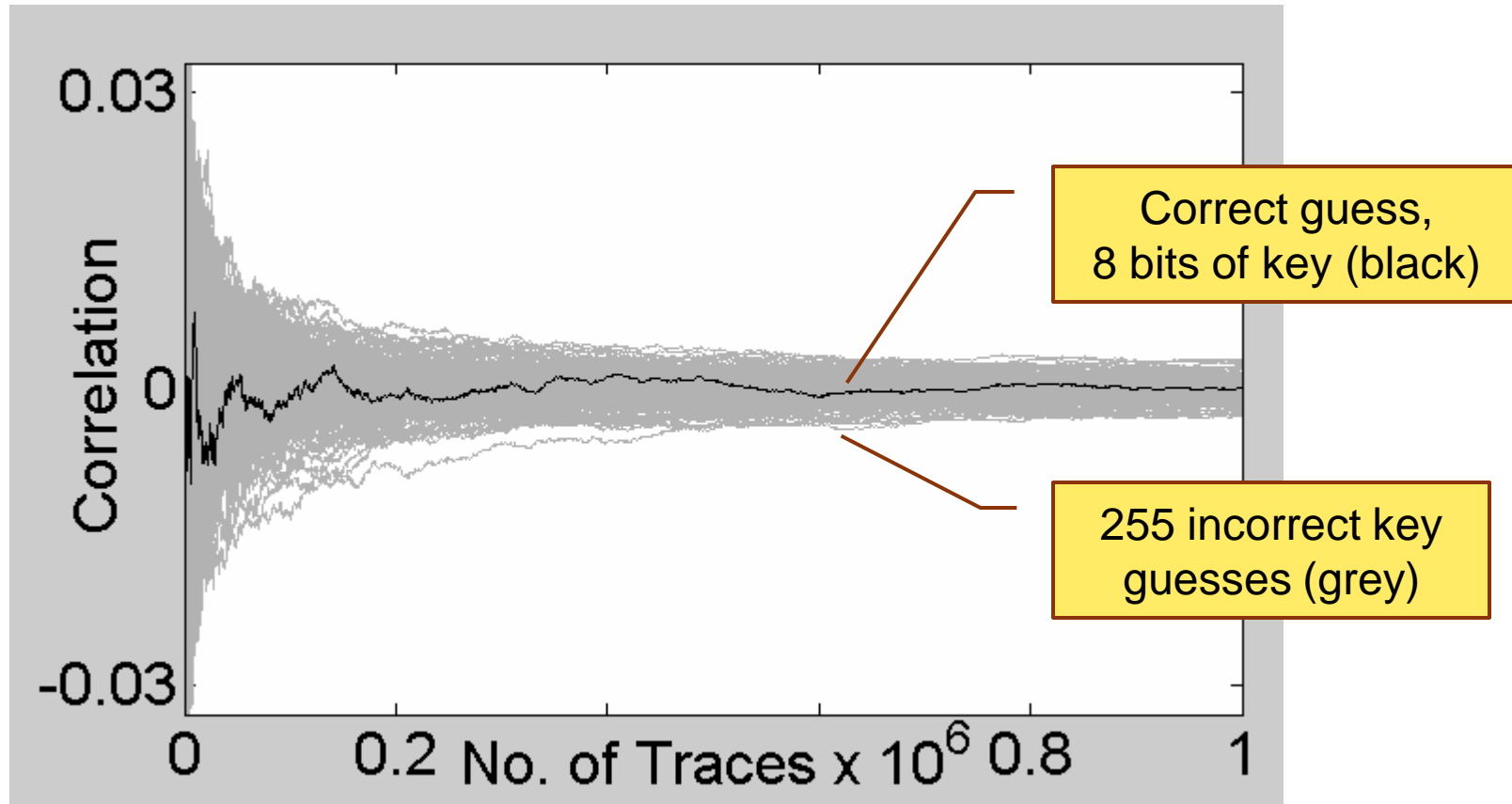
# Correlation Power Trace for 256 key guesses With Countermeasures



With countermeasures, the correlation for a correct key guess is virtually indistinguishable from that of any of the wrong keys

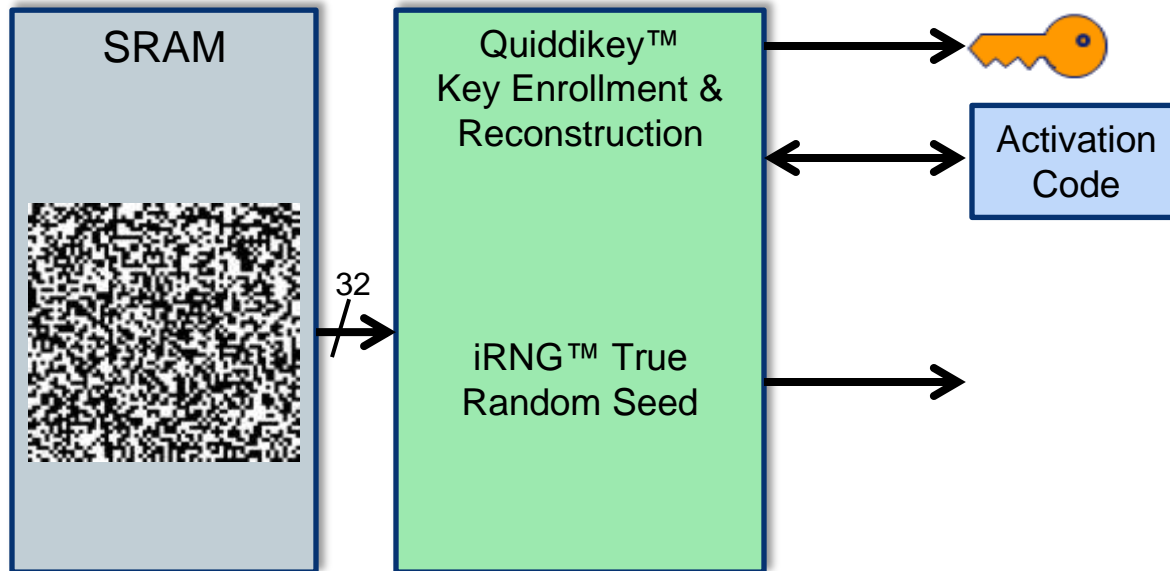
<sup>1</sup> Correlation vs. time estimated from 1,000,000 power measurements

# Correlation vs. Number of Measurements With Countermeasures



With countermeasures, the correlation for a correct key guess is virtually indistinguishable from that of any of the wrong keys, even for a large number of measurements (1,000,000 shown)

# SRAM PUF Concept



Cryptographic Keys

- Full entropy
- Fixed/static

&

True Random Seed

- Full entropy
- Dynamic

# Hardware Intrinsic Security – Soft HW or FW

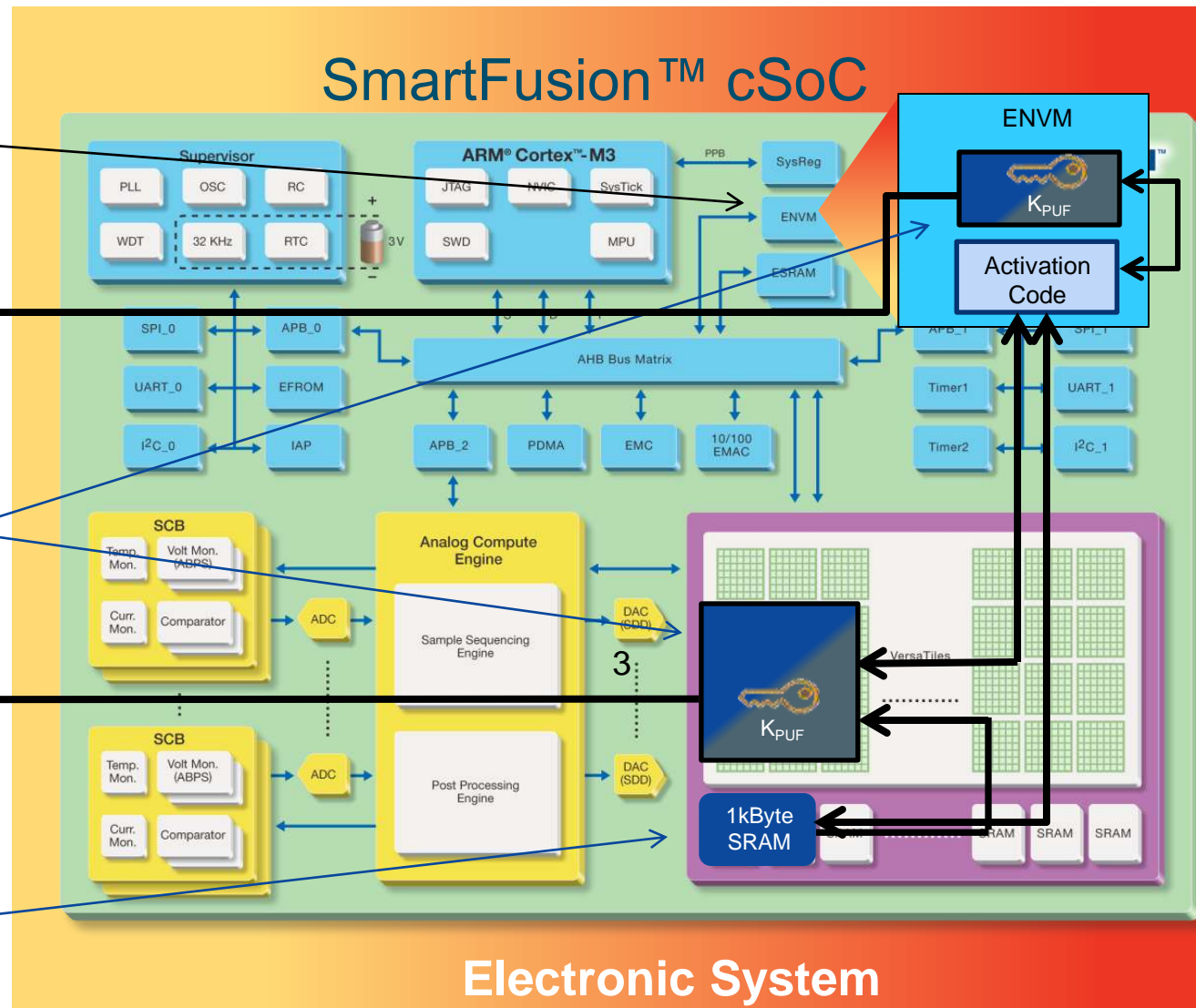
Store activation code in flash memory during enrollment; use during key regeneration

$K_{PUF}$

Intrinsic-ID's Quiddikey™ has both gate-level and firmware implementations to chose from

$K_{PUF}$

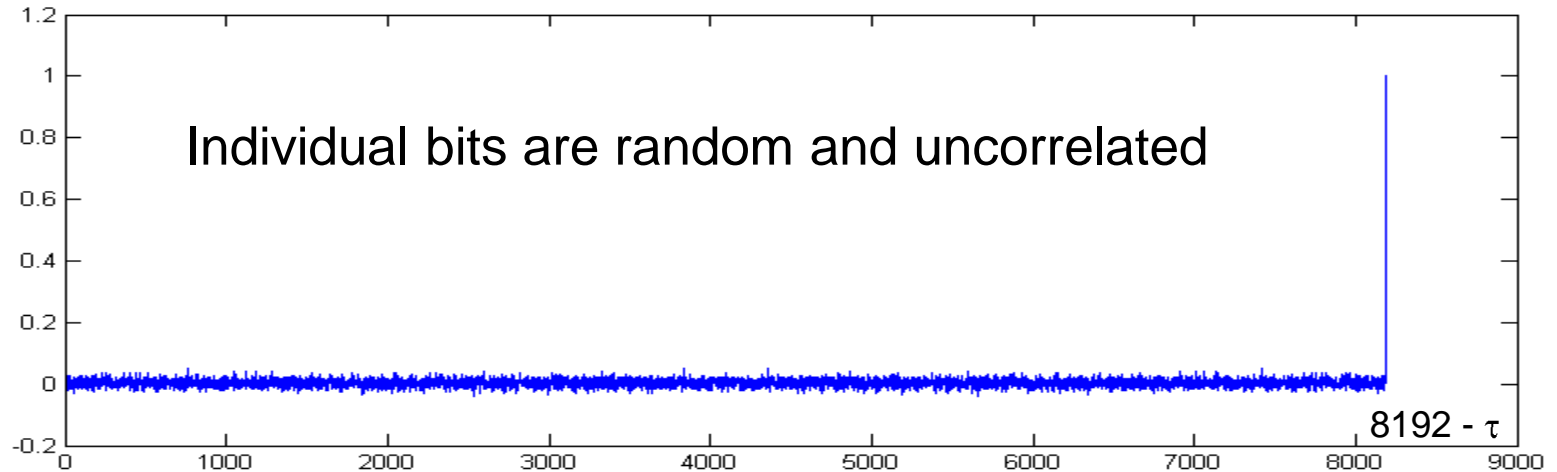
“Fingerprint” obtained using dedicated SRAM blocks



Electronic System

# Preliminary Test Results

Normalized Auto-correlation of 8192 bits of SRAM (SmartFusion™ A2F500)



100% - Hamming Difference (%)

Experiment #

- 1. 144138: **Bd1 -- BLK0**
- 2. 145432: **Bd1 -- BLK0**
- 3. 145445: **Bd1 -- BLK1**
- 4. 145943: **Bd1 -- BLK0**
- 5. 154624: **Bd2 -- BLK0**
- 6. 155111: **Bd2 -- BLK0**

	1	2	3	4	5	6
1	100%	95.6%	49.4%	96.4%	50.7%	50.4%
2		100%	49.6%	95.1%	51.0%	50.6%
3			100%	49.4%	49.9%	49.7%
4				100%	50.8%	50.3%
5					100%	91.9%
6						100%

- Same SRAM readings are highly correlated from turn-on to turn-on (>90%)
- Different SRAM readings are highly uncorrelated (50% ±1%)
  - Same device, different block; or different device, same relative block

# Trends

# Predicting the Future of cSoC



“It's tough to make predictions, especially about the future.”

“The future ain't what it used to be.”

*Yogi Berra*

# Security-cSoC Architecture

- Three major digital blocks:

## System Controller

- Dedicated pgm'ing controller
- Cryptographic Accelerators and functions (e.g., AES)
- Secure management of Programming Key(s)
- DPA and other countermeasures

## Analog

- Optional – Some models only

## Microprocessor Sub-System (MSS)

- CPU (e.g., Cortex®-M3)
- eSRAM & eNVM
- Hardened Peripherals (more & more)

## FPGA

- LUTs and FFs; interconnect
- Tightly-coupled SRAM blocks
- Math blocks
- Peripherals & Interfaces

# cSoC Design Security Trends

- More use models
  - Support for both security conscious and security agnostic users
- Better designed cryptography & protocols
  - Especially, improved authentication
  - Mitigation against protocol-level attacks
  - Improved key management with more user options
- Improved integration and automation
  - Self-contained field-upgrade engine for FPGA and/or FW (eNVM)
- Ever improving resistance to various forms of tampering
  - Strong resistance to Differential Power Analysis will eventually be the norm



# Data Security Trends

- Not just performance-vs-area any more
  - Security options provide another axis for decisions
  - De-commoditization of cryptographic IP cores
- Growing Eco-system of third-party HW and FW security IP
  - DPA-resistant crypto algorithms
  - Middle-ware and network security protocol stacks
  - Countermeasure cores
  - New security primitives, e.g., SRAM-PUF for non-volatile key storage
- Opportunity for new business models
  - For example, key management services
- Military-grade firmware obfuscation
- Higher integration with fewer external components
  - Security boundary approaching the single-chip level
- Higher overall security levels attainable for those with need
  - Approaching nation-state level

# More Security Applications Addressed by cSoC

- Expanding security market
  - Both high-bandwidth and low-bandwidth applications
- Not just high-volume cost-sensitive consumer applications any more
  - Such as those served by low-cost security microcontrollers
  - Higher prices tolerated if security is delivered
- Expanding military applications
  - Fewer custom security ASICs
- Higher integration
  - Greatly expanded I/O requirements compared to SmartCard
- Biggest Trend:
  - The Internet of Things
  - Security becoming ubiquitous (e.g., medical devices, automobiles)

# Some Security Applications - Commercial

Network Security



Digital Rights Management  
(e.g., Flight Video)



Gaming



Secure Flash Storage



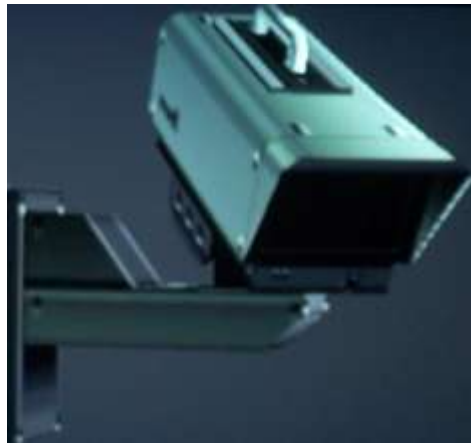
Point-of-Sale Terminals /  
PIN-entry Devices

Copyright 2011 Microsemi Corporation



Cash Registers

# Some Security Applications – Commercial, cont.



Security Cameras

## Biometric Identification



Card Readers



Security Systems



Wireless Robots



Mobile Multi-Switcher Installation - Front Cab of First Responder Vehicle

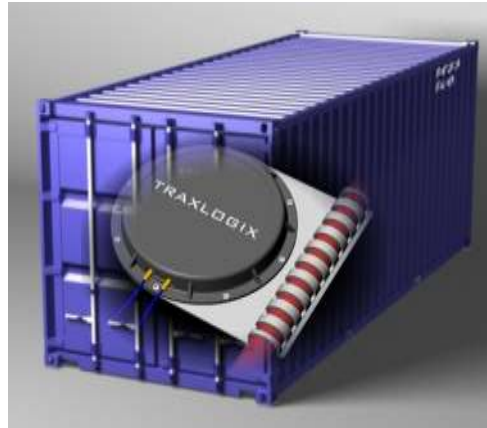
Commercial Radios

# Some Security Applications – Industrial/Medical

## Smart Grid Sensors/Meters



## Container Tracking



## Wireless Patient Data



## Programmable Logic Controllers



## Fleet/Driver Tracking



## Smart Grid Thermostat



## Wireless Water Meter



## Wireless Asthma Inhaler

# Some Security Applications - Consumer



Internet / Smart Grid Refrigerator



Internet Connected Devices (e.g., Radios)



## Security Tokens

- Key management
- Encryption
- Authentication



Set-Top Box

# Some Security Applications - Military

Future Force Warrior

Heads-up Display

Data Glove



Tactical Radios / Secure Communications



Ruggedized  
Navigation/Intelligence  
System

Storage



# Key Take-aways

---

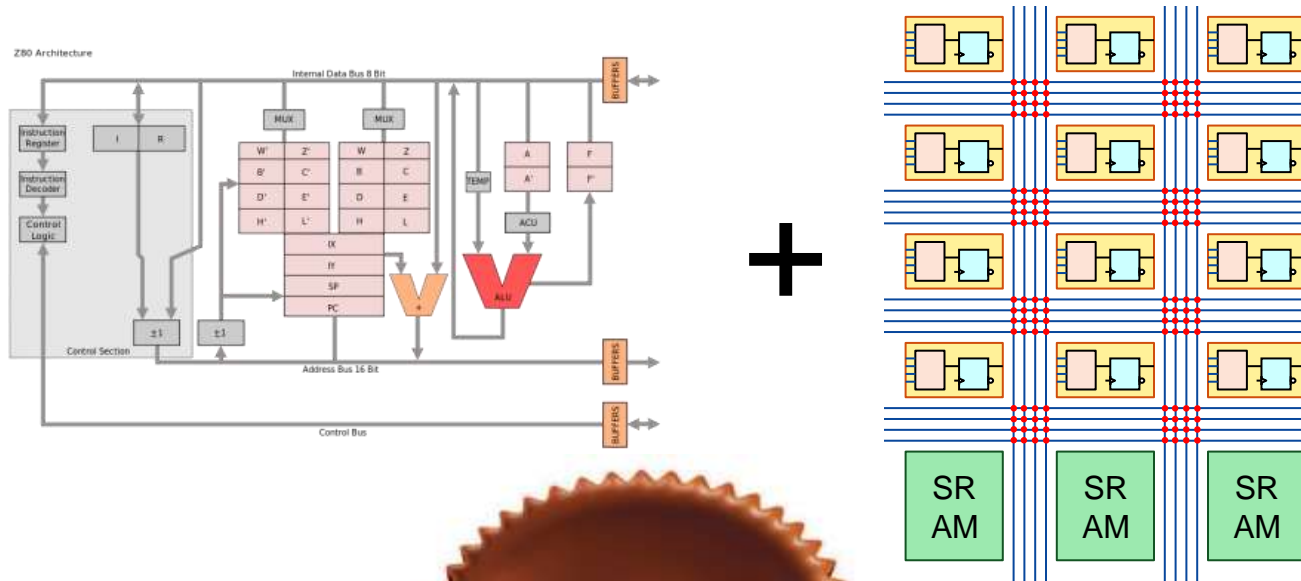
- By marrying two prominent computational architectures, CPU & FPGA, a more capable device was formed: the cSoC
  - Can handle complex algorithms
  - Can perform computations in parallel – tremendous computing power
  - Highly scalable over several orders of magnitude
  
- Security attributes, common in SmartCards and Defense ICs, are increasingly being applied to the cSoC
  - cSoC security is approaching and will eventually exceed requirements for a single-chip security boundary
  - For example, strong DPA resistance

# Key Take-aways, cont.

- These trends are creating a new class of security IC: the cSoC
  - Scalable computing power, starting above that of most low-cost security microcontrollers and extending several orders of magnitude
  - Plenty of I/O, including support for high-bandwidth interfaces
  - Dedicated fixed-function programming and cryptography co-processor
- Security is becoming ubiquitous
  - Higher security levels are being required in every application
  - More devices are connected to the Internet: The Internet of Things
  - Fielded devices have to provide their own security
- The technology and the market are coming together for the cSoC

# Enjoy!

- Customizable System-on-Chip = cSoC = MCU + FPGA



It's a tasty combination!

Thank you for your attention!

# Acronyms used in this presentation

ADC	Analog-to-Digital Converter	I/F	Interface	SRAM	Static Random-Access Memory
AES	Advanced Encryption Std.	I/O	Input/Output	UART	Universal Asynchronous Receiver/Transmitter
CISC	Complex Instruction Set Computer	IP	Intellectual Property	USB	Universal Serial Bus
CPLD	Complex PLD	ISP	In-circuit Programming	VANET	Vehicle-Area Network
CPU	Central Processing Unit	LUT	Look-up Table	μP	Micro-Processor
cSoC	customizable SoC	MCU	Micro-Controller Unit	μs	micro-second
DPA	Differential Power Analysis	MMU	Memory Management Unit		
DRBG	Deterministic Random Bit Generator	NIOS	® Altera; a soft RISC CPU		
DSP	Digital Signal Processing	NPU	Network Processor Unit		
ECC	Elliptic Curve Cryptography	NVM	Non-Volatile Memory		
EDAC	Error Detection & Correction	OTP	One-Time Programmable		
EM	Electro-Magnetic	PCI	Peripheral Component Interconnect		
eNVM	Embedded NVM	PLD	Programmable Logic Device		
FIB	Flip-Flop	PLL	Phase-Locked Loop		
FPGA	Field Programmable Gate Array	PWM	Pulse-Width Modulator		
FW	Firmware	RISC	Reduced Instruction-Set Computer		
GPU	Graphic Processing Unit	ROM	Read-only Memory		
HIS	Hardware Intrinsic Security	RSA	Rivest-Shamir-Adelmann (cryptographic algorithm)		
HW	Hardware	S-Box	Substitution-Box		
IAP	In-Application Programming	SoC	System-on-Chip		