NXP LPC5500 SERIES OVERVIEW & ARCHITECTURE

Jiunn Yang

Field Application Engineer, FAE

TECHNOLOGY DAYS

April 2020

Public– NXP, the NXP logo, and NXP secure connections for a smarter world are trademarks of NXP B.V.
All other product or service names are the property of their respective owners. © 2019 NXP B.V.

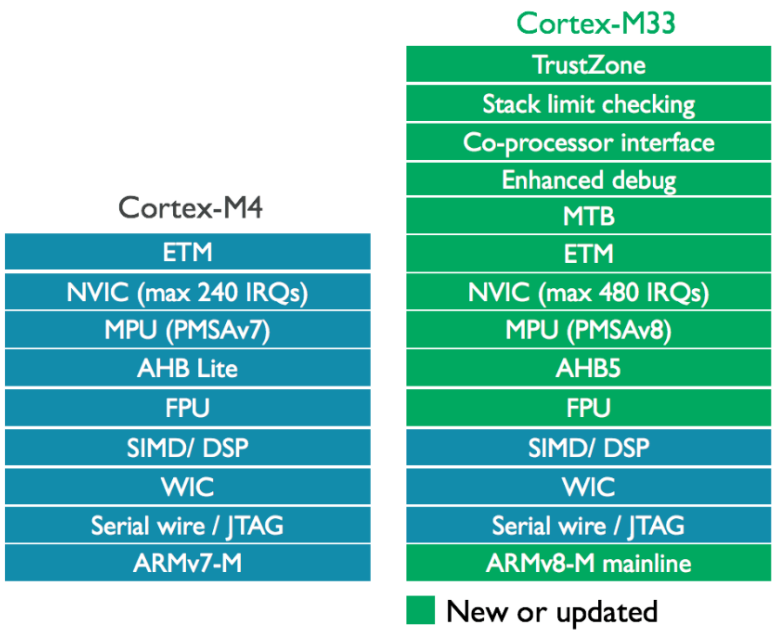
Agenda

- ARM Cortex-M33
- LPC5500
- Coprocessor
- Advanced Security Subsystem
- Power Management
- System Infrastructure
- Enablement

ARM Cortex-M33

Cortex-M33 Key Features

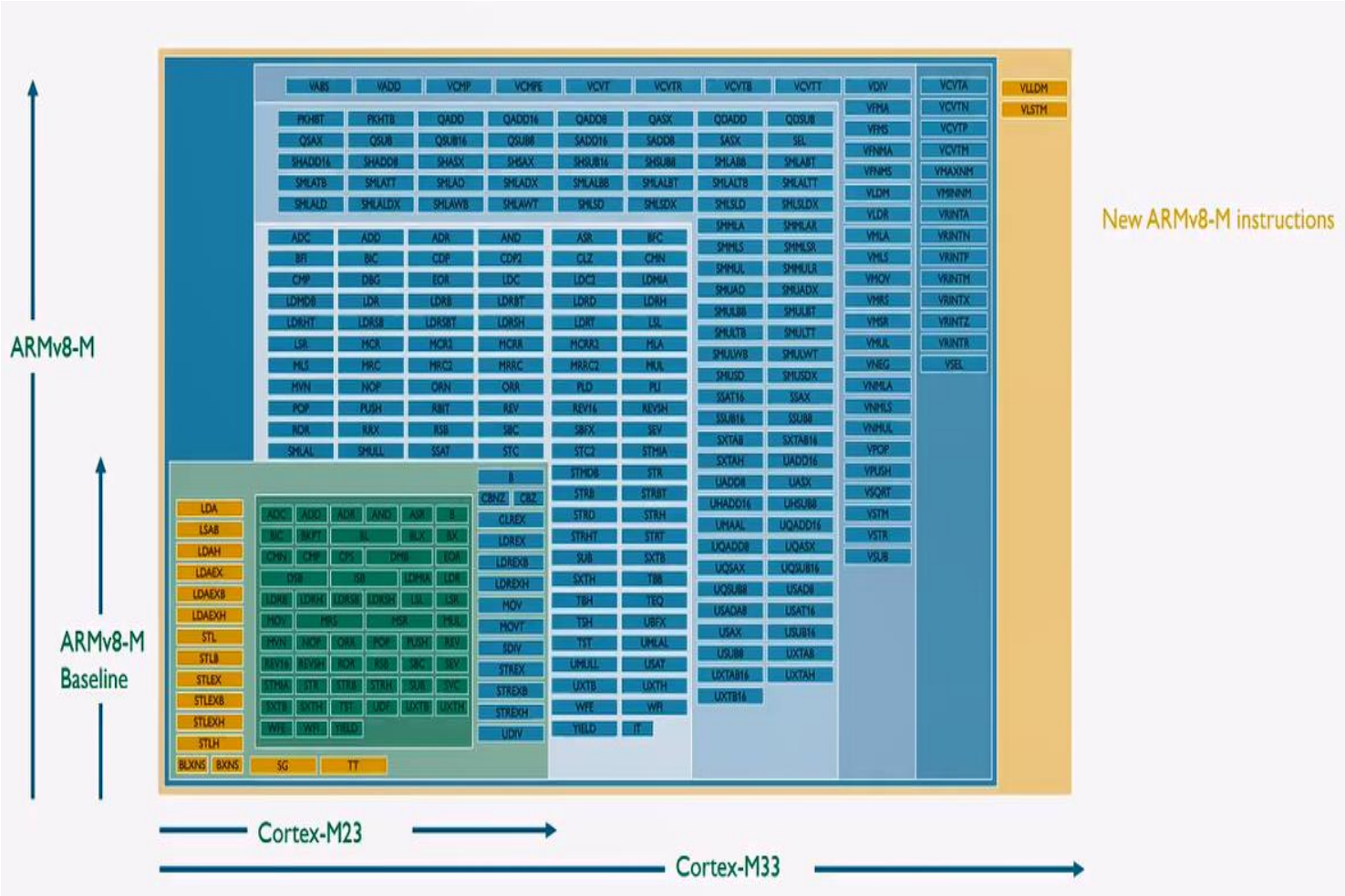
- **Armv8-M** architecture mainline
- **2 stage** instruction **pipeline** w/ early completion of common arithmetic instructions enabling more efficient execution
  - 3 stages for complex arithmetic operations
  - Limited **dual-issues** of common 16-bit instruction pairs
- **Unaligned access supported**
- **Load acquire, store release** instructions (C11 atomic variable support)
- Optional **TrustZone** – system-wide, secure resource isolation for trusted software & co-processor extensions to embedded MCU applications
- New style **MPU** programmer's model w/ PMSAv8, improved flexibility in MPU region definition
- Optional **Floating** point extension architecture v5 w/ 3 stages pipeline, one MAC/3 cycles
- Better debug capability – enhancements in breakpoint and watchpoint units
- Optional **coprocessor** support for hardware acceleration



	Dhrystone DMPIS/MHz (v2.1)	CoreMark/MHz (v1.0)
Cortex-M3	1.25	3.32
Cortex-M4	1.25	3.40
Cortex-M33	**1.50**	**3.86**

Cortex-M33 Instruction Set

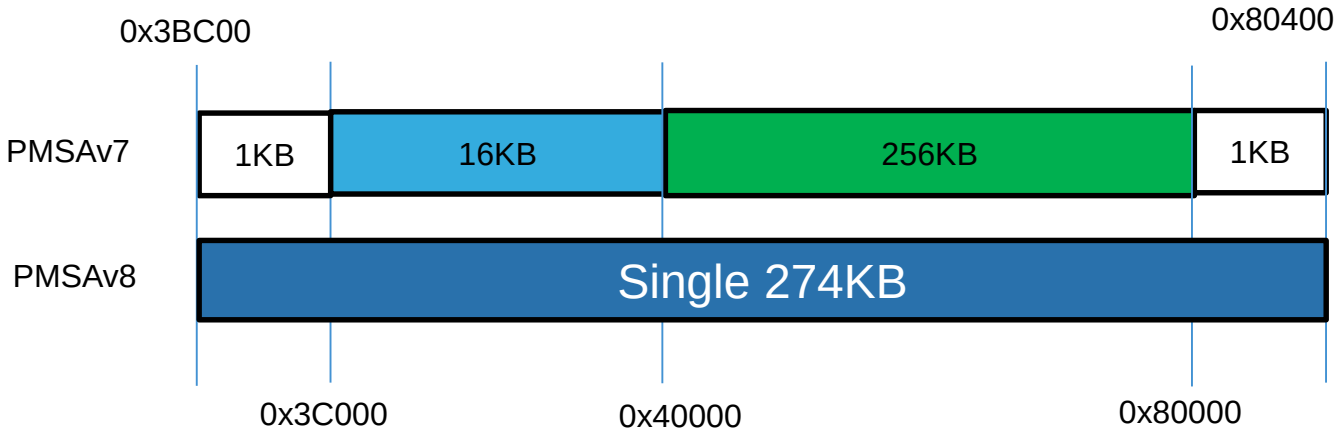
- **Implement T32 instruction set**
- **Extension to ARMv7-M**
  - Mix of 16-bit/32-bit instruction
  - Added Load Acquire/Store Release instruction
- **Optional security extension**
  - Functional calls between security states (SG, BXNS, BLXNS)
  - Memory protection unit address queries (TT)



Cortex-M33 MPU

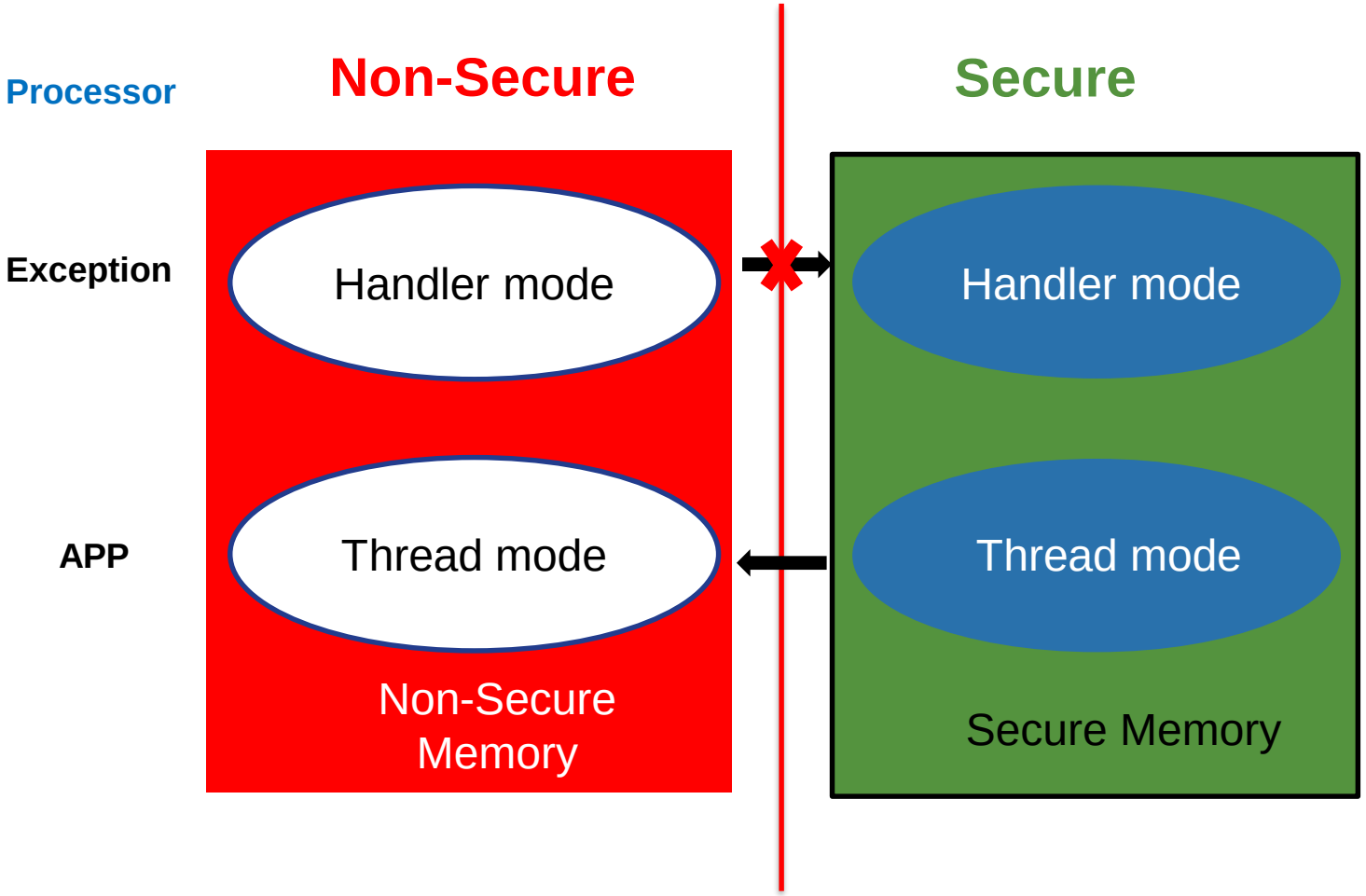
- Allow privileged software to control access to physical memory
- Partition physical memory into configurable regions w/ smallest region size = 32B
- Region address/size - No need 2^n aligned
- Change memory region type and attributes
- Change peripheral and device regions to executable
- Define region memory access permissions
- Monitor instruction and data accesses to memory
- Trigger a fault/exception when access violation occurs

PMSAv8 vs PMSAv7



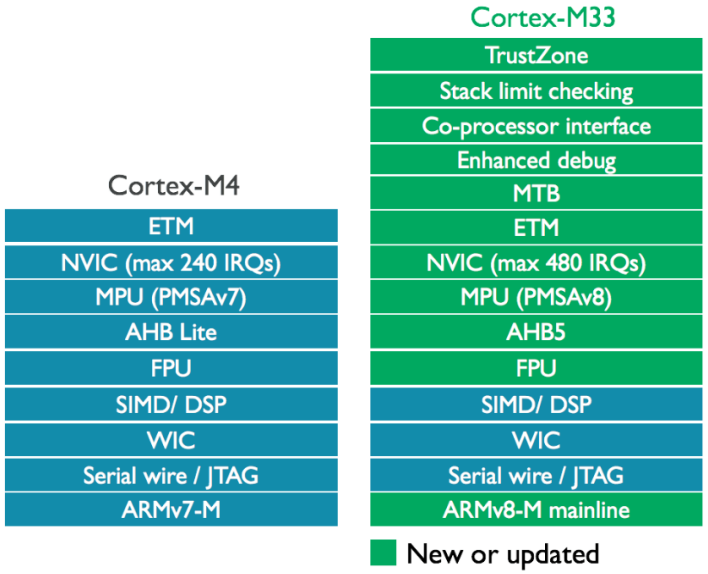
Cortex-M33 TrustZone

- **Optional Security Extension, optimized for energy efficient MCU**
- **Full isolation of system resource to Secure/Non-Secure by SAU/IDAU**
  - Secure memory: secure code + data (secure stack, heap, any other secure data)
  - Non-Secure Callable (**NSC**) memory: entry functions for Non-Secure programs to access Secure functions
- **Processor states in Secure/Non-Secure, dependent on the memory attribute**
- **Secure software is highly trusted**
  - Has access to more system resource
  - Protected from access by non-trusted code
- **Secure code can access both Secure & Non-Secure information whereas Non-Secure programs can only access Non-Secure information**
- **Non-secure code can call Secure lib only via NSC**



LPC5500

Industry's ONLY Full ArmV8-M Implementation



Key Features and Comparisons

- **Nearly 20% performance improvement over Cortex-M4 based MCUs** (over 60% vs Cortex-M0) with redesigned pipeline - up to two instructions per clock cycle

	Cortex-M0+	Cortex-M23	Cortex-M3	Cortex-M4	Cortex-M33
DMIPS/MHz	**0.95**	0.98	1.25	1.25	**1.50**
CoreMark®/MHz	**2.46**	2.50	3.32	3.40	**4.02**

Prelim. Data from Arm for Cortex-M33 implementation at 40LP (9-track, typical 1.1v, 25°C)

- **TrustZone for system-wide, secure resource isolation** enabling trusted runtime execution and physical protection in embedded MCU applications

- **Tightly coupled accelerators with coprocessor interface & extensions** (Arm's single precision FPU along with NXP accelerators)

NXP LPC5500 MCU Series

Roadmap

COMMON PLATFORM ARCHITECTURE FOR COMPLETE SCALABILITY
AREA & PERFORMANCE EFFICIENT

Advanced Efficiency & Integration

LPC55S6x

150 MHz Cortex-M33 (dual, PQ)
Up to 640KB Flash/320KB SRAM
SDIO
Enhanced Security with TrustZone (‘S’ version)

Balanced

LPC55S2x/2x

150 MHz Cortex-M33
Up to 512KB Flash/256KB SRAM
SDIO
Enhanced Security without TrustZone (‘S’ version)

Entry

LPC55S1x/1x

100 MHz Cortex-M33
Up to 256KB Flash/96KB SRAM
Single CAN-FD
Enhanced Security with TrustZone (‘S’ version)

2019 | 2019 | 2020

Draft – Subject to change

NXP LPC5500 MCU Series

Common Platform Architecture for Complete Scalability

Common features across families

- FS/HS USB with PHY, 50MHz SPI, up to 8/10 Serial Interfaces (FlexComm), plus I3C interface (LPC557x/8x families)
- 5x 32b Timers, SCTimer, and FlexPWM (on LPC553x/7x/8x)
- Up to 2Msps 16-bit SAR ADC, Comparator, Temperature Sensor and RTC (time stamp/tamper on LPC553x/7x/8x)
- 1.8 to 3.6V, -40 to 105 °C

LPC5500 Family	Samples [Launch]	Memory	Tgt Max Freq	Dual Core	Security Features	DSP Accel.	USB*	SDIO	CAN-FD*	10/100 ENET	Graphics Accel.	Analog	Serial Interface
Graphics/HMI LPC558x/S8x	**Q3-20**	Up to 1-2MB Flash, >=512KB SRAM	≥150 MHz Opt TZ	Yes	Opt.	Yes	FS&HS	Yes	2x	1x	Yes	2x 2Msps 16b ADC 2x 12b DAC 3x OpAmps	10x FlexComm HS SPI, I3C
Memory Exp. LPC557x/S7x	**Q3-20**	Up to 1-2MB Flash, >=512KB SRAM	150 MHz Opt TZ	Yes	Opt.	Yes	FS&HS	Yes	2x	1x	-	2x 2Msps 16b ADC 2x 12b DAC 3x OpAmps	10x FlexComm HS SPI, I3C
Efficiency LPC55S6x	**Q4-18** [Mar-19]	Up to 640KB Flash, 320KB SRAM	150 MHz ~~100 MHz~~ (with TZ)	Yes	Yes	Yes	FS&HS	Yes	-	-	-	1x 1Msps 16b ADC	8x FlexComm, HS SPI
Adv. Analog LPC553x/S3x	**Q1-20**	Up to 256KB Flash, 96KB SRAM	150 MHz Opt TZ	-	Opt.	Yes	FS Only	Yes	1x	-		2x 2Msps 16b ADC 2x 12b DAC 3x OpAmps	8x FlexComm, HS SPI
Mainstream LPC552x/S2x	**Q3-19** [Sep-19]	Up to 512KB Flash, 256KB SRAM	150 MHz (No TZ)	-	Opt.	-	FS&HS	Yes	-	-	-	1x 1Msps 16b ADC	8x FlexComm, HS SPI
Entry LPC551x/S1x	**Q4-19** [Feb-20]	Up to 256KB Flash, 96KB SRAM	150 MHz Opt TZ	-	Opt.	-	FS&HS	-	1x	-	-	1x 2Msps 16b ADC	8x FlexComm, HS SPI
Streamlined LPC550x	**2021**	0KB Flash, 96KB SRAM	100 MHz Opt TZ	-	-	-	FS&HS	Yes	-	-	-	1x 1Msps 16b ADC	8x FlexComm, HS SPI

- **HS USB/CAN-FD not available on all part numbers within the family, check data sheet for specific configurations*

NXP LPC5500 MCU Series

Pin Compatibility Across Packages

LPC5500 Family	Memory	WL CSP	QFN 64/48	QFP 64	QFP 100	QFP 144	BGA 98	BGA 196
Graphics/HMI LPC558x/S8x	Up to 1.5MB Flash, 512KB SRAM				X	X		X
Memory Exp. LPC557x/S7x	Up to 1.5MB Flash, 512KB SRAM				X	X		X
Efficiency LPC55S6x	Up to 640KB Flash, 320KB SRAM			X	X	X	X	
Adv. Analog LPC553x/S3x	Up to 256KB Flash, 96KB SRAM		X	X	X		X	
Mainstream LPC552x/S2x	Up to 512KB Flash, 256KB SRAM		X	X	X		X	
Entry LPC551x/S1x	Up to 256KB Flash, 96KB SRAM		X	X	X		X	
Streamlined LPC550x	0KB Flash, 96KB SRAM		X	X	X			

Upon Customer Request

Pin Compatibility

Subject to Change
(X = justification required)

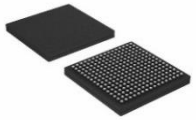
LQFP

LQFP144 vs MaxQFP144

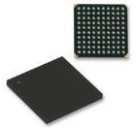
HLQFP100
14x14mm-x,y, 1.4mm- z
0.5mm pitch

HTQFP64
10x10mm-x,y, 1.0mm- z
0.5mm pitch

BGA



BGA196
TBD



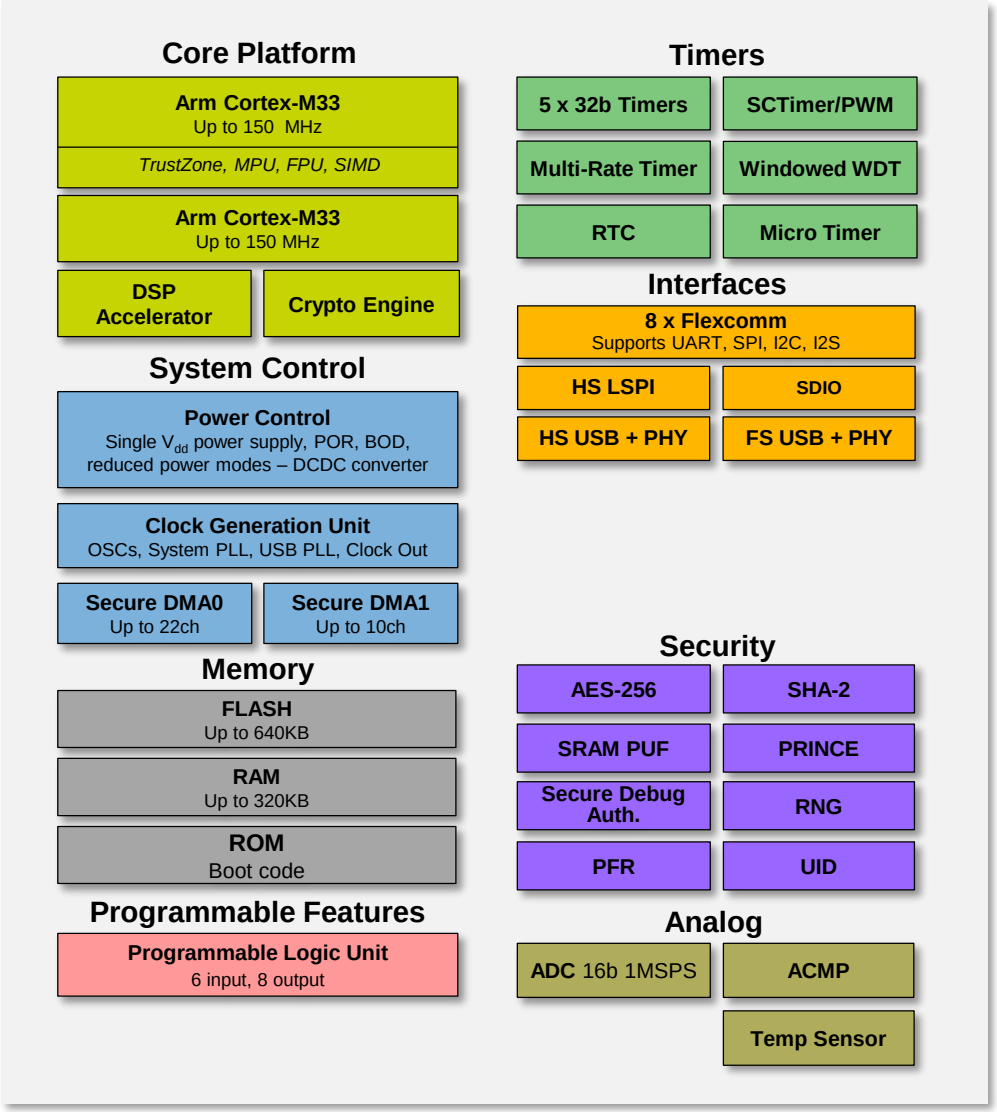
VFBGA98
7x7mm-x,y, 0.86mm- z
0.5mm pitch

QFN

HVQFN64
9x9mm-x,y, 1.0mm- z
0.5mm pitch

QFN48
7x7mm-x,y, 1.0mm- z
0.5mm pitch

LPC55S6x Product Block Diagram



Subject to Change, NDA Required

Core Platform

- Up to 150MHz Cortex-M33
  - TrustZone, MPU, FPU, SIMD
- Up to 150MHz Cortex-M33
- Coprocessors
  - DSP Accelerator
  - Crypto Engine
- Multilayer Bus Matrix

Memory

- Up to 640KB FLASH (PFR included)
- Up to 320KB RAM
- 128KB ROM

Timers

- 5 x 32b Timers
- SCTimer/PWM
- Muiti-Rate Timer
- Windowed Watchdog Timer
- RTC
- Micro Timer

Interfaces

- USB High-speed (H/D) w/ on-chip HS PHY
- USB Full-speed (H/D), Crystal-less
- SDIO, Support 2 cards
- 1 x High-Speed SPI up to 50MHz
- 8 x Flexcomms support up to 8x SPI, 8x I2C, 8x UART, 4x I^2S channels (total 8 instances)

Advanced Security

- Protected Flash Region (PFR)
- AES-256 HW Encryption/Decryption Engine
- SHA-2
- SRAM PUF for Key Generation support
- PRINCE – Real-time Encrypt/Decrypt for flash data
- Secure debug authentication
- RNG
- Secure boot

Analog

- 1 x 16b ADC, 10ch, 1MSPS
- Analog Comparator
- Temperature Sensor

Packages

- HLQFP100, 14x14mm
- VFBGA98, 7x7mm
- HTQFP64, 10x10mm

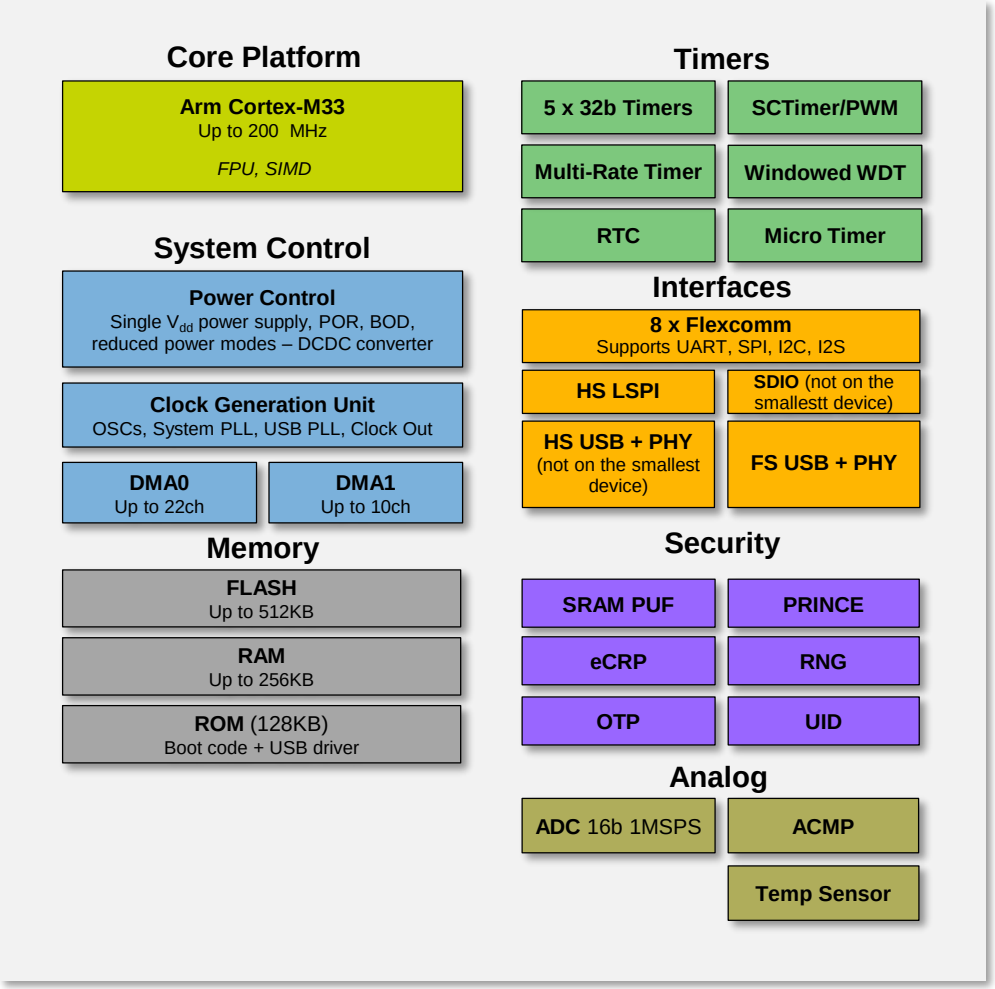
Other

- Programmable Logic Unit
- Buck DC-DC
- Operating voltage: 1.8 to 3.6V
- Temperature range: -40 to 105 °C

LPC55S6x Orderable Part Numbers

	CPU0	CPU1	PowerQuad	Casper	Flash	RAM	Secure Boot	TrustZone	PRINCE	SRAM PUF	SDIO	USB	GPIO
LPC55S69JBD100 (QFP100)	Y	Y	Y	Y	640	320	Y	Y	Y	Y	Y	HS+FS	64
LPC55S66JBD100 (QFP100)	Y	Y	Y	Y	256	144	Y	Y	Y	Y	Y	HS+FS	64
LPC55S69JEV98 (BGA98)	Y	Y	Y	Y	640	320	Y	Y	Y	Y	Y	HS+FS	64
LPC55S66JEV98 (BGA98)	Y	Y	Y	Y	256	144	Y	Y	Y	Y	Y	HS+FS	64
LPC55S69JBD64 (QFP64)	Y	Y	Y	Y	640	320	Y	Y	Y	Y	Y	HS+FS	36
LPC55S66JBD64 (QFP64)	Y	Y	Y	Y	256	144	Y	Y	Y	Y	Y	HS+FS	36

LPC552x/S2x Product Overview



Core Platform

- Up to 150MHz Cortex-M33
- Multilayer Bus Matrix

Memory

- Up to 512KB FLASH
- Up to 256KB RAM
- 128KB ROM

Timers

- 5 x 32b Timers
- SCTimer/PWM
- Muiti-Rate Timer
- Windowed Watchdog Timer
- RTC
- Micro Timer

Interfaces

- USB High-speed (H/D) w/ on-chip HS PHY (not in the 128k version)
- USB Full-speed (H/D), Crystal-less
- SDIO, Support 2 cards (not in the 128k version)
- 1 x High-Speed SPI up to 50MHz
- 8 x Flexcomms support up to 8x SPI, 8x I2C, 8x UART, 4x I^2S channels (total 8 instances)

Advanced Security ('S' version only)

- Protected Flash Region (PFR)
- AES-256 HW Encryption/Decryption Engine
- SHA-2
- SRAM PUF for Key Generation support
- PRINCE – Real-time Encrypt/Decrypt for flash data
- Secure debug authentication
- RNG
- Secure boot

Analog

- 16b ADC, 10ch, 1MSPS
- Analog Comparator
- Temperature Sensor

Packages

- HLQFP100, 14x14mm
- VFBGA98, 7x7mm
- HTQFP64, 10x10mm

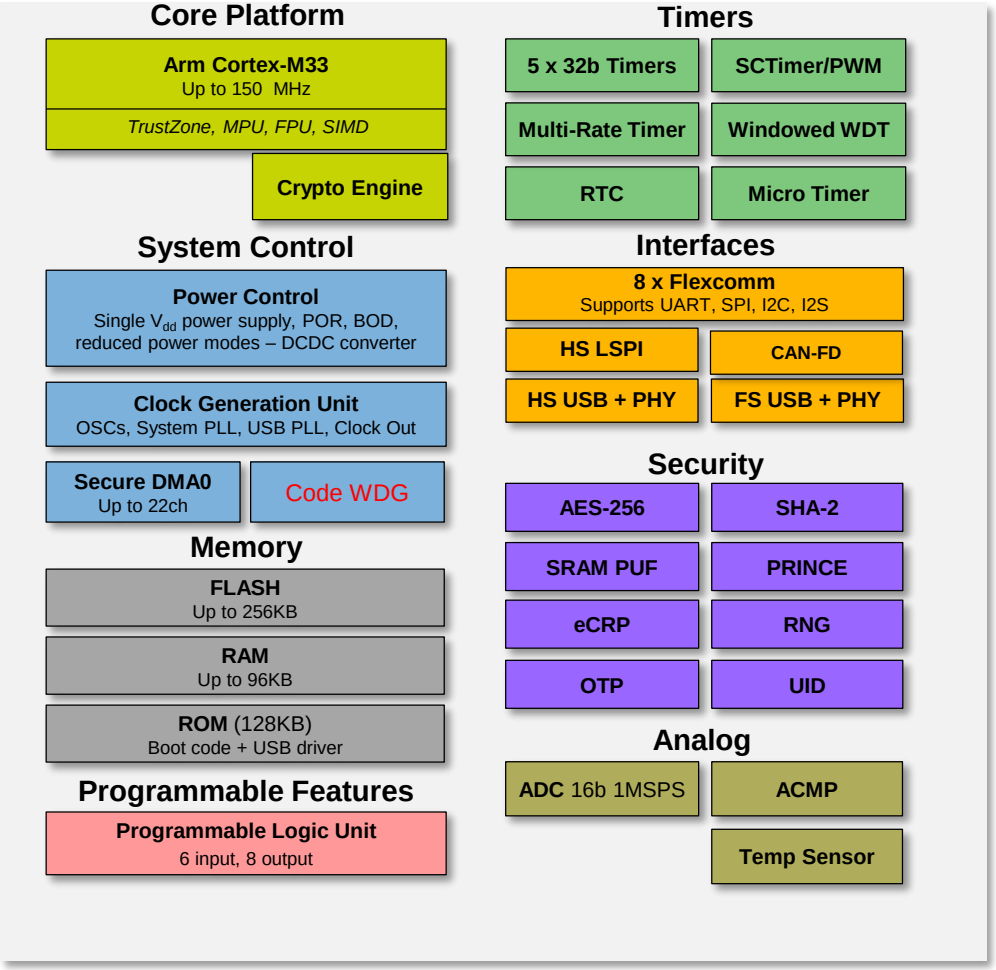
Other

- Buck DC-DC
- Operating voltage: 1.8 to 3.6V
- Temperature range: -40 to 105 °C

LPC552x/S2x Orderable Part Numbers

Part number	CPU0	CPU1	PowerQuad	Casper	Flash	RAM	Secure Boot	TrustZone	PRINCE	SRAM PUF	SDIO	USB	GPIO
LPC55S28JBD100 (QFP100)	Y	N	N	Y	512	256	Y	N	Y	Y	Y	HS+FS	64
LPC55S28JEV98 (BGA98)	Y	N	N	Y	512	256	Y	N	Y	Y	Y	HS+FS	64
LPC55S28JBD64 (QFP64)	Y	N	N	Y	512	256	Y	N	Y	Y	Y	HS+FS	36
LPC55S26JBD100 (QFP100)	Y	N	N	Y	256	144	Y	N	Y	Y	Y	HS+FS	64
LPC55S26JEV98 (BGA98)	Y	N	N	Y	256	144	Y	N	Y	Y	Y	HS+FS	64
LPC55S26JBD64 (QFP64)	Y	N	N	Y	256	144	Y	N	Y	Y	Y	HS+FS	36
LPC5528JBD100 (QFP100)	Y	N	N	N	512	256	N	N	N	N	Y	HS+FS	64
LPC5528JEV98 (BGA98)	Y	N	N	N	512	256	N	N	N	N	Y	HS+FS	64
LPC5528JBD64 (QFP64)	Y	N	N	N	512	256	N	N	N	N	Y	HS+FS	36
LPC5526JBD100 (QFP100)	Y	N	N	N	256	144	N	N	N	N	Y	HS+FS	64
LPC5526JEV98 (BGA98)	Y	N	N	N	256	144	N	N	N	N	Y	HS+FS	64
LPC5526JBD64 (QFP64)	Y	N	N	N	256	144	N	N	N	N	Y	HS+FS	36

LPC551x/S1x Product Overview



Core Platform

- Up to 150MHz Cortex-M33
  - TrustZone ('S' version), MPU, FPU, SIMD
- Coprocessors
  - Crypto Engine
- Multilayer Bus Matrix

Memory

- Up to 256kB FLASH
- Up to 96kB RAM
- 128kB ROM

Timers

- 5 x 32b Timers
- SCTimer/PWM
- Multi-Rate Timer
- Windowed Watchdog Timer
- RTC
- Micro Timer

Interfaces

- USB Full-speed (H/D), Crystal-less
- 1 x High-Speed SPI up to 50MHz
- 8 x Flexcomms support up to 8x SPI, 8x I2C, 8x UART, 4x I^2S channels (total 8 instances)
- CAN FD

Analog

- 16b ADC, 10ch, 2MSPS
- Analog Comparator
- Temperature Sensor

Advanced Security ('S' version only)

- Protected Flash Region (PFR)
- AES-256 HW Encryption/Decryption Engine
- SHA-2
- SRAM PUF for Key Generation support
- PRINCE – Real-time Encrypt/Decrypt for flash data
- Secure debug authentication
- TRNG
- Secure boot (flash re-map)
- Code WDG

Packages

- HLQFP100, 14x14mm
- VFBGA98, 7x7mm
- HTQFP64, 10x10mm

Other

- Programmable Logic Unit
- Buck DC-DC
- Operating voltage: 1.8 to 3.6V
- Temperature range: -40 to 105 °C

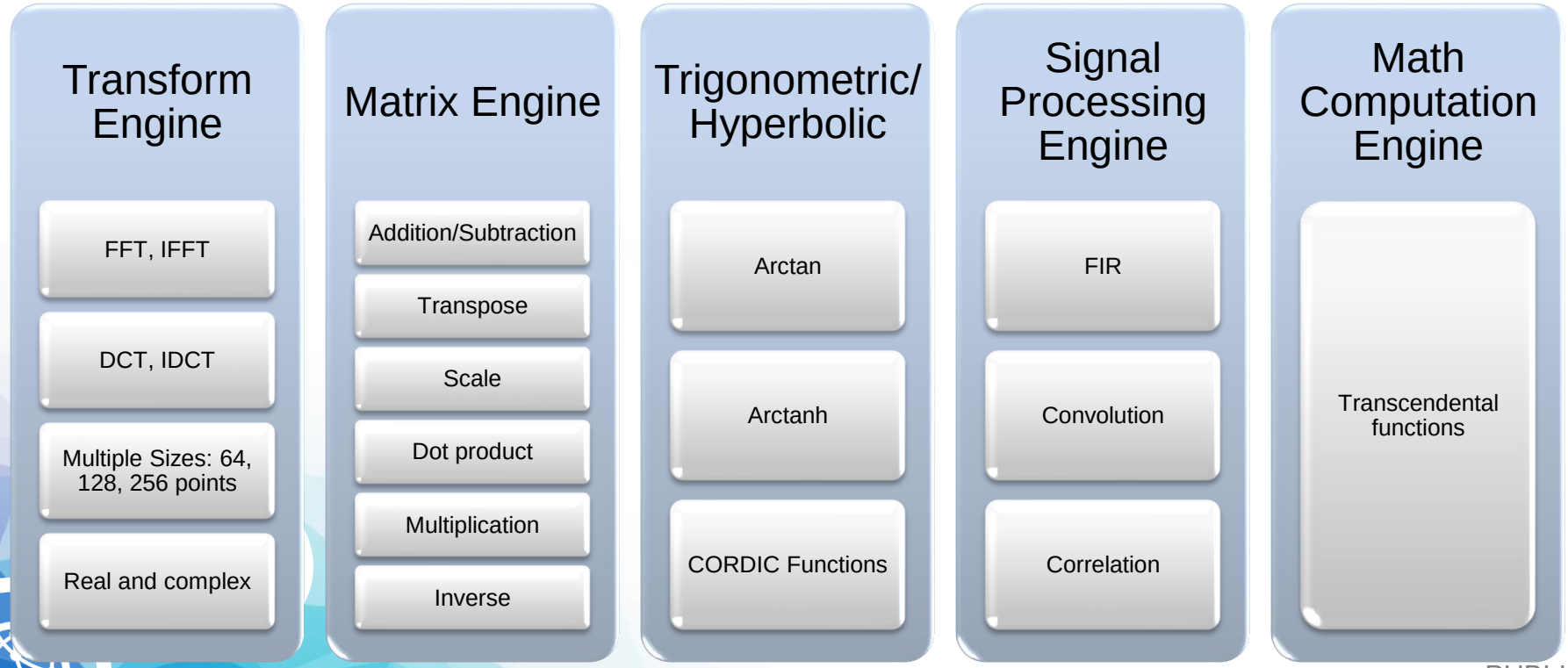
Subject to Change, NDA Required

LPC551x/S1x Orderable Part Numbers

Part number	CPU0	CPU1	PowerQuad	Casper	Flash	RAM	Secure Boot	TrustZone	PRINCE	SRAM PUF	SDIO	USB	CAN2.0/ CAN-FD	GPIO
LPC55S16JBD100 (QFP100)	Y	N	N	Y	256	96	Y	Y	Y	Y	N	HS+FS	CAN-FD	64
LPC55S16JEV98 (BGA98)	Y	N	N	Y	256	96	Y	Y	Y	Y	N	HS+FS	CAN-FD	64
LPC55S16JBD64 (QFP64)	Y	N	N	Y	256	96	Y	Y	Y	Y	N	HS+FS	CAN-FD	36
LPC55S14JBD100 (QFP100)	Y	N	N	Y	128	80	Y	Y	Y	Y	N	HS+FS	CAN-FD	64
LPC55S14JBD64 (QFP64)	Y	N	N	Y	128	80	Y	Y	Y	Y	N	HS+FS	CAN-FD	36
LPC5516JBD100 (QFP100)	Y	N	N	N	256	96	N	N	N	N	N	HS+FS	CAN-FD	64
LPC5516JEV98 (BGA98)	Y	N	N	N	256	96	N	N	N	N	N	HS+FS	CAN-FD	64
LPC5516JBD64 (QFP64)	Y	N	N	N	256	96	N	N	N	N	N	HS+FS	CAN-FD	36
LPC5514JBD100 (QFP100)	Y	N	N	N	128	80	N	N	N	N	N	HS+FS	CAN-FD	64
LPC5514JBD64 (QFP64)	Y	N	N	N	128	80	N	N	N	N	N	HS+FS	CAN-FD	64
LPC5512JBD100 (QFP100)	Y	N	N	N	64	48	N	N	N	N	N	FS	CAN 2.0	64
LPC5512JBD64 (QFP64)	Y	N	N	N	64	48	N	N	N	N	N	FS	CAN 2.0	36

NXP's PowerQuad Hardware Accelerator

- HW accelerator for frequently used math and signal processing computations
- ARM CMSIS-DSP API provides standardization for DSP code running on Cortex-M cores. Co-processors can leverage this API
- 15x more efficienct than Cortex-M33 running CMSIS-DIP lib for FFT/IFFT (~50x faster than generic FFT C-code running on Cortex-M33)



Key Advantages

- Energy consumption reduction for DSP tasks
- Fast implementation for 'lego' blocks of DSP processing
- Can Operate in parallel with Arm Cortex-M33 Core
- No need for wasting RAM lookup tables

NXP LPC5500 MCU Series

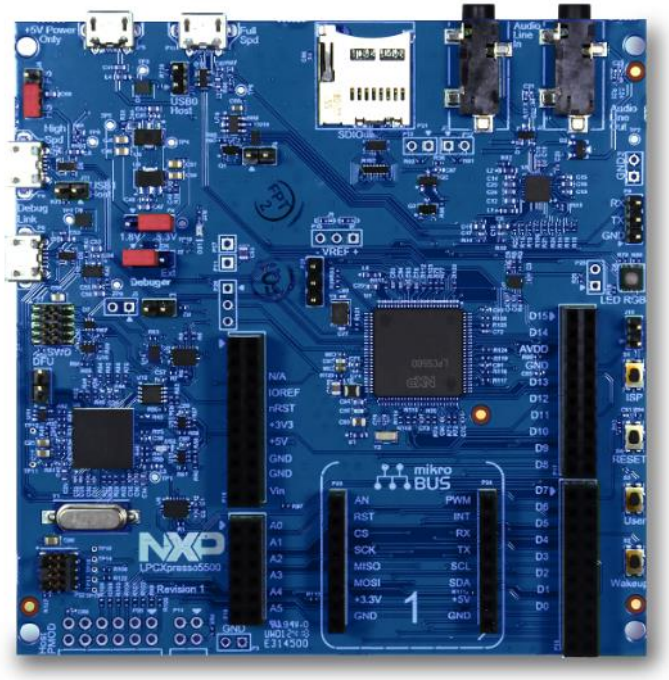
MCUXpresso Software & tools ecosystem

Complimentary with Extensive Support

- MCUXpresso SDK
- MCUXpresso IDE
- MCUXpresso Config Tools

Hardware Platform for Ease of Development

- On-board debug circuit
- PCB Layout, Schematic and Board Files Available



LPC55S69-EVK

ARM KEIL Microcontroller Tools

IAR SYSTEMS

SEGGER

Simplify secure embedded development; Reduce time to market.

LPC5500 MCU Series

Highlights

Main Highlights of LPC5500

- World's First General Purpose Cortex-M33 based MCU in the market Today
- Leading Performance Efficiency with 32uA/MHz in Active Mode
- PowerQuad DSP for math intensive functions
- Advanced security featuring TrustZone, SRAM PUF, real-time encryption/decryption, etc
- Pin and Software Compatibility across the LPC5500 MCU Series
- Robust Enablement with MCUXpresso Software & Tools

Start your Development Now! www.nxp.com/LPC55S69-EVK

NXP LPC5500 MCU Series

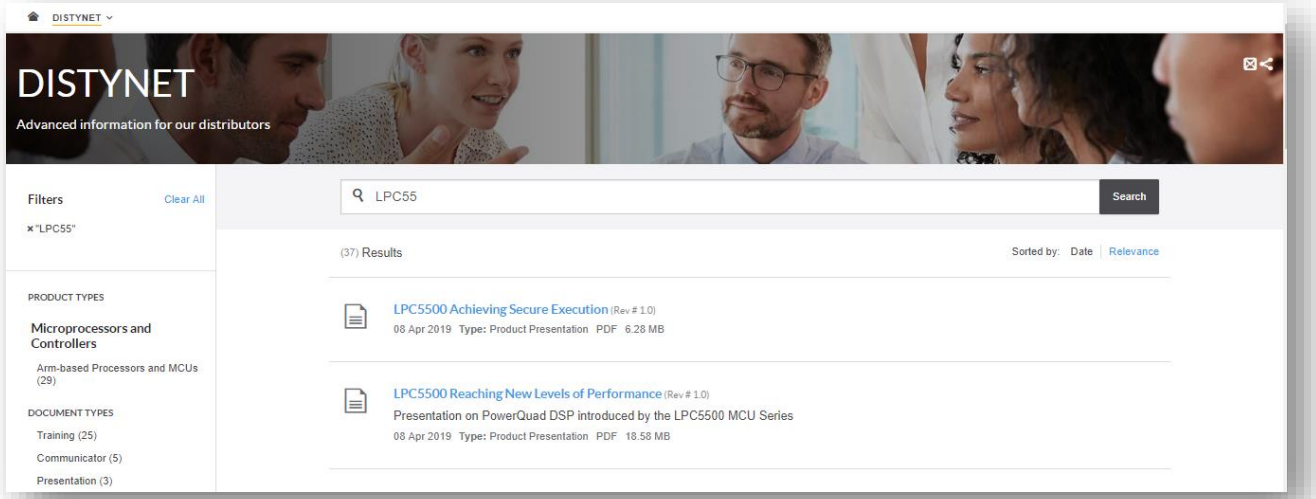
References to Learn More!

Technical Support

https://community.nxp.com/welcome

Visit NXP MCUs Online

www.NXP.com/MCU



- LPC5500 Six Pack
- LPC5500 Technical Marketing
- LPC5500 Performance Efficiency w/ PowerQuad DSP Accelerator
- LPC5500 Security Architecture

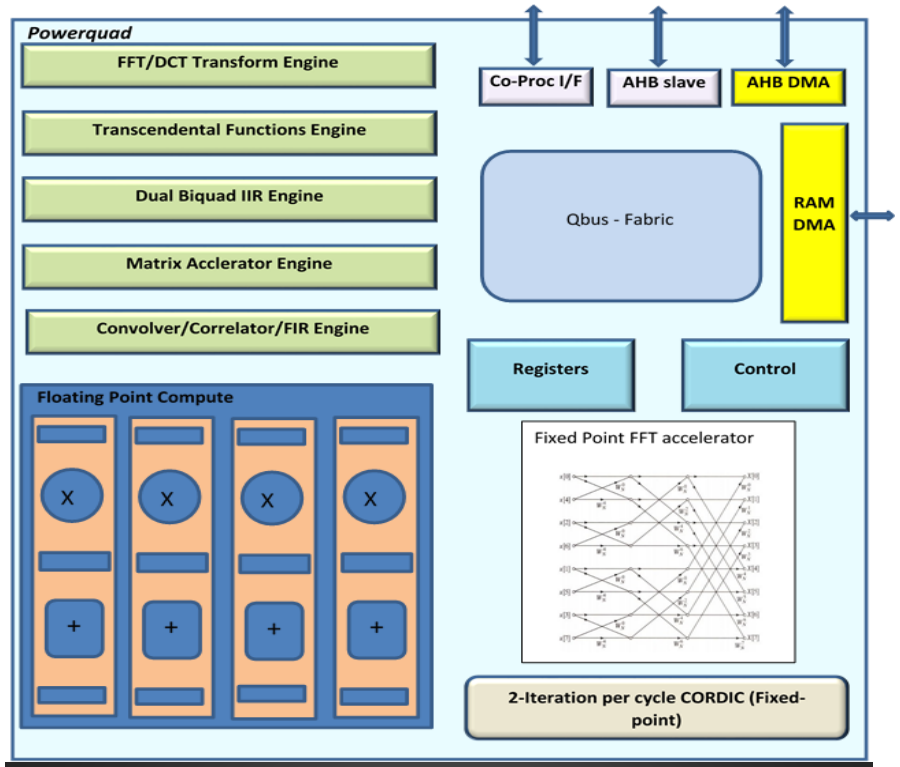
Search **LPC55** on DistyNet for more presentations and videos!

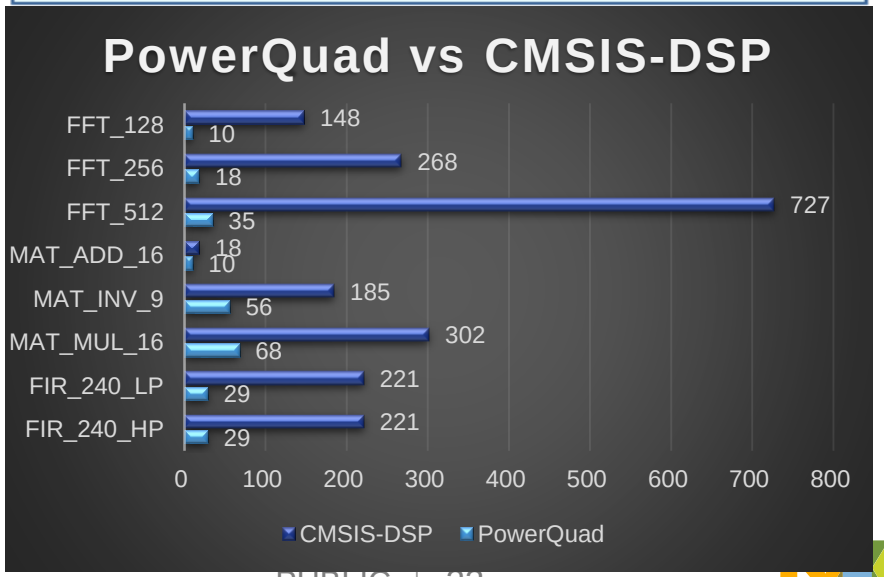
Coprocessor

PowerQuad

Powerful DSP accelerator

- 4x Single Precision Floating MAC
- AHB DMA - read/write data for input/computations/results
- RAM DMA – to handle 128bit wide RAM for input/computations/results
- Qbus fabric – Data pipe to route requests from machines to RAM or AHB (supports up to 5 data handled in parallel)
- Co-processor Interface for tightly coupled opcodes (**use two MACs**, can run two in parallel)
- Accelerate mathematical calculation/DSP
  - **FFT**/iFFT/DCT/iDCT machine
  - Matrix (add, sub, dot, prod, mult, inverse, transpose, scale)
  - Convolution/Correlation/**FIR, biquad(x)**
  - sin(x), cos(x), ln(x), e^(x), e^(-x),1/(x),1/sqrt(x), sqrt(x)
  - Arctan / Arctanh (but also customizable to compute any CORDIC function)
- **CMSIS-DSP APIs** to simplify customer code portability

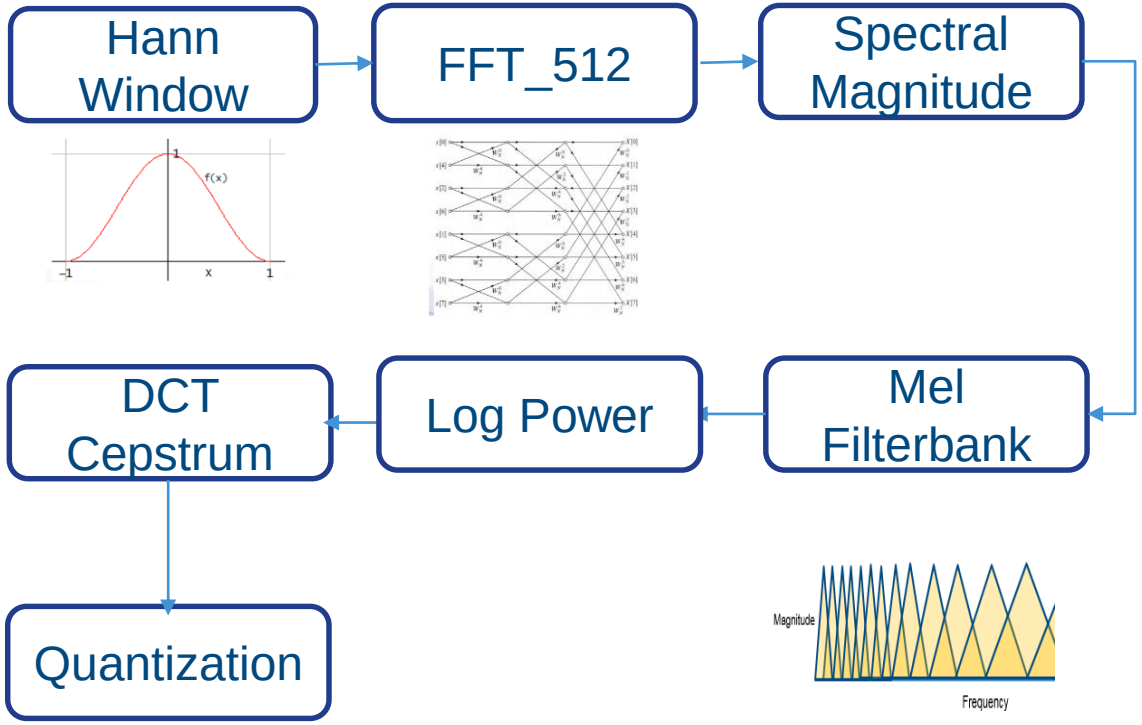




PowerQuad

Speech Recognition feature extraction using Mel Frequency Cepstral Coefficient (MFCC)

- Audio data: 16-bit fixed point, 16KHz
- MFCC operation < **11000** cycles (at a rate of 100 MFCCs per second)
- Only consume less than **1.1MIPS, around an order of magnitude faster than CM33**



PowerQuad Performance

- Performance speed up by running CM33+PQ (Vector function)

Function	Format	MACs	PQ cycles	CM33 cycles	Ratio	Vector cycles	Vector Ratio
sqrt(x)	Fixed/ Float	2	6	131 (14 for FPU)	21.83 (2.33)	4.5	29.11 (3.1)
1/sqrt(x)	Fixed/ Float	2	6	145 (14 for FPU)	24.17 (2.33)	4.5	32.22 (3.1)
sin(x)	Fixed/ Float	2	8	37 (117 for accurate+)	4.63 (14.63)	5 (23.4)	7.4 (15.81)
cos(x)	Fixed/ Float	2	8	37 (117 for accurate+)	4.63 (14.63)	5 (23.4)	7.4 (15.81)
biquad(x)	Fixed/ Float	2	5	15	3.00	4.5	3.33
y/x	Float	2	6	13	2.17	4.5	2.89
1/x	Fixed/ Float	2	6	12	2.00	4.5	2.67
ln(x)	Fixed/ Float	2	6	92	15.33	4.5	20.44
e^{x}	Fixed/ Float	2	7	121	17.29	5	24.20
e^{-x}	Fixed/ Float	2	7	122	17.43	5	24.40

PowerQuad Performance

- FFT/DCT Engine

Function	CM33 (ms)	PQ (ms)	Ratio	Notes
arm_rfft_q15	683	80	8.54	Input data length = 512, 10K times
arm_rfft_q31	1640	80	20.50	
arm_cfft_q15	1236	87	14.21	
arm_cfft_q31	2267	89	25.47	
arm_ifft_q15	1237	87	14.22	
arm_ifft_q31	2273	87	26.13	
arm_dct4_q15	1634	396	4.13	Input data length = 512
arm_dct4_q31	2760	410	6.73	

PowerQuad Performance

- Convolution/Correlation/FIR

Function	CM33 (ms)	PQ (ms)	Ratio	Notes
arm_conv_q15	219	19.8	11.06	Data A length = 5, Data B length = 5 10K times
arm_conv_q31	114	19.8	5.76	
arm_conv_f32	116	19.8	5.86	
arm_correlate_q15	236	20.40	11.57	Data A length = 5, Data B length = 5 10K times
arm_correlate_q31	122	19.8	6.16	
arm_correlate_f32	117	19.8	5.91	
arm_fir_q15	213	46.20	4.61	16 input data, 12 taps, 10K times
arm_fir_q31	476	45.60	10.44	
arm_fir_f32	266	45.6	5.83	

PowerQuad Performance

- Matrix Engine

Function	CM33 (ms)	PQ (ms)	Ratio	Notes
arm_mat_add_q15	28	15	1.87	16 x 16, 10K times
arm_mat_add_q31	51	15	3.40	
arm_mat_add_f32	60	15	4.00	
arm_mat_sub_q15	28	15	1.87	
arm_mat_sub_q31	50	15	3.33	
arm_mat_sub_f32	61	16	3.81	
arm_mat_mult_q15	584	66	8.85	
arm_mat_mult_q31	878	65	13.51	
arm_mat_mult_f32	982	65	15.11	
arm_mat_trans_q15	41	19	2.16	
arm_mat_trans_q31	42	19	2.21	
arm_mat_trans_f32	40	22	1.82	
arm_mat_scale_q15	49	18	2.72	
arm_mat_scale_q31	69	18	3.83	
arm_mat_scale_f32	44	15	2.93	
arm_mat_inverse_f32	549	138	3.98	9 x 9, 10K times

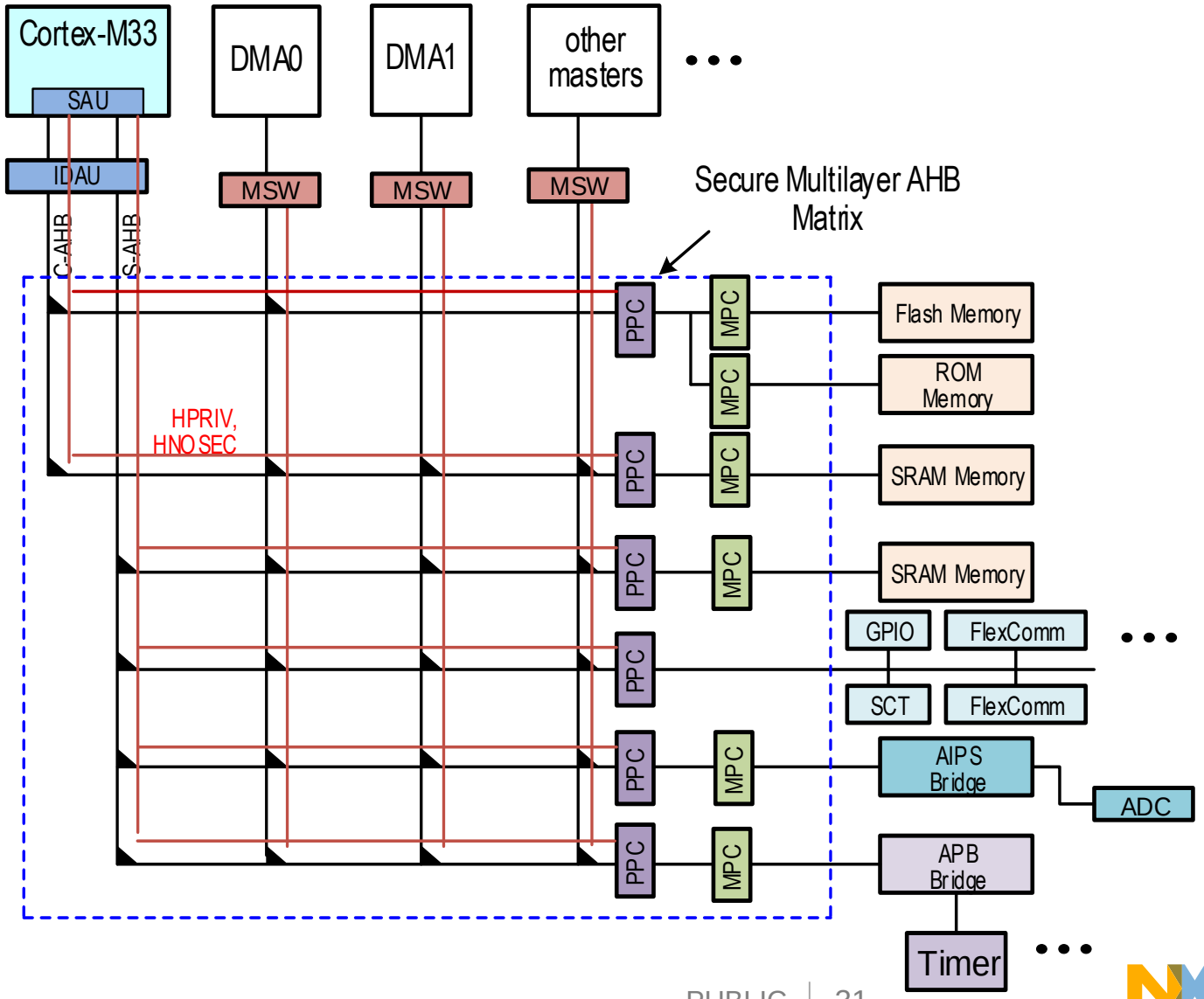
Advanced Security subsystem

LPC55Sxx Security Architecture Summary

Security Goal	Security Blocks on LPC55Sxx
Counterfeit protection	UUID (RFC4122), Chip unique Root Key(PUF), DICE (unique tracking), PRINCE (Encrypted flash)
Secure Communication	CASPER for asymmetric crypto, AES 256 Engine(ECB, CTR, CBC), SHA Hashing Engine(SHA1, SHA2), TRNG
Data Confidentiality	PUF (key store), AES-256 Engine, CASPER
Firmware Update	ROM API with SB file processing,
System Integrity	TrustZone for armv8M, Pole/anti-pole checks, Secure boot, DICE
Onboarding	Flexible provision with PUF keys, DICE based PKI, RoT Public Key Hash in FFR for trust establishment

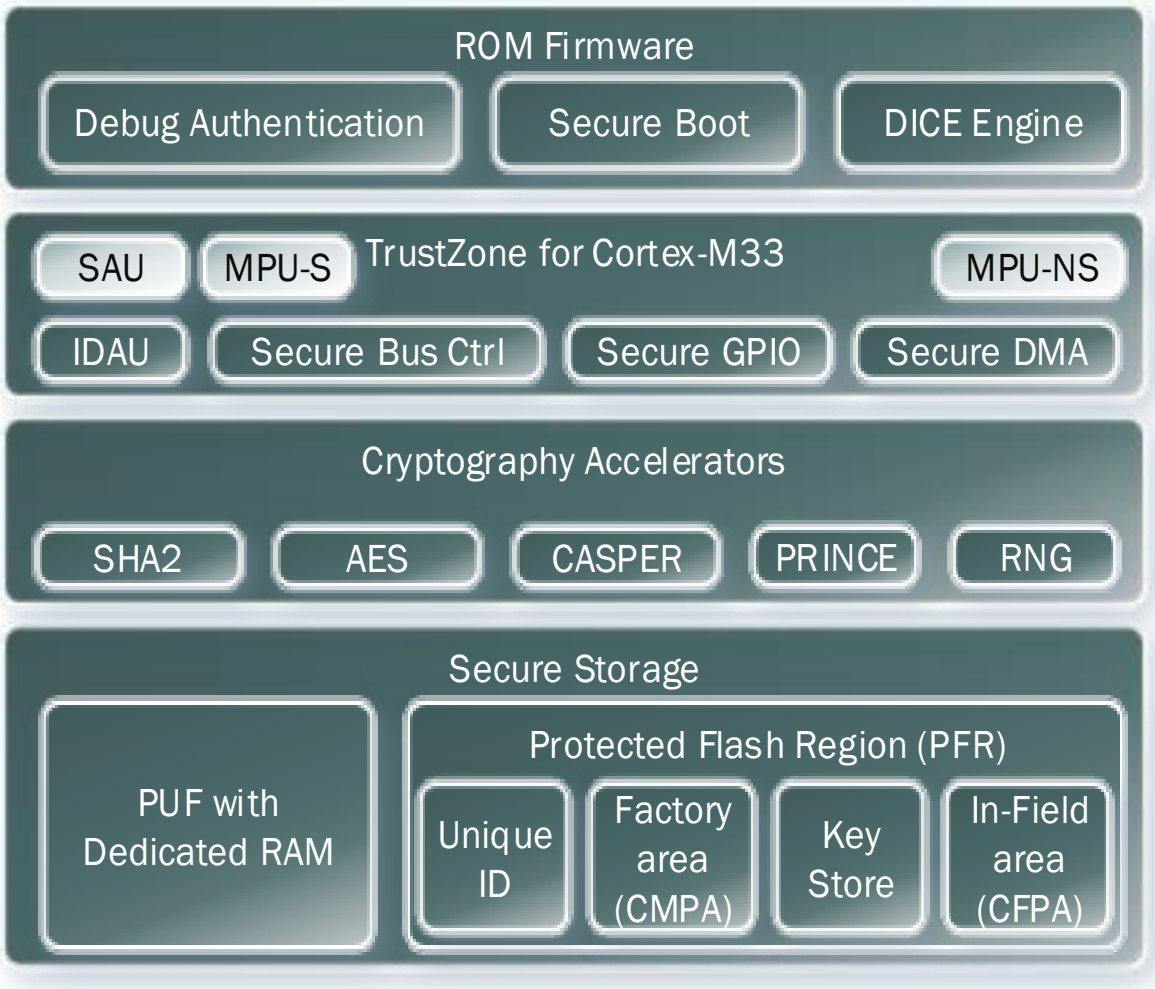
LPC55Sxx Trusted Execution Environment

- Secure AHB Control consists of 2nd layer of security protection at system level
  - Memory Protection Checker (MPC)
  - Peripheral Protection Checker (PPC)
  - Master Security Wrapper (MSW)
- TrustZone + Secure AHB Control = Trusted Execution Environment



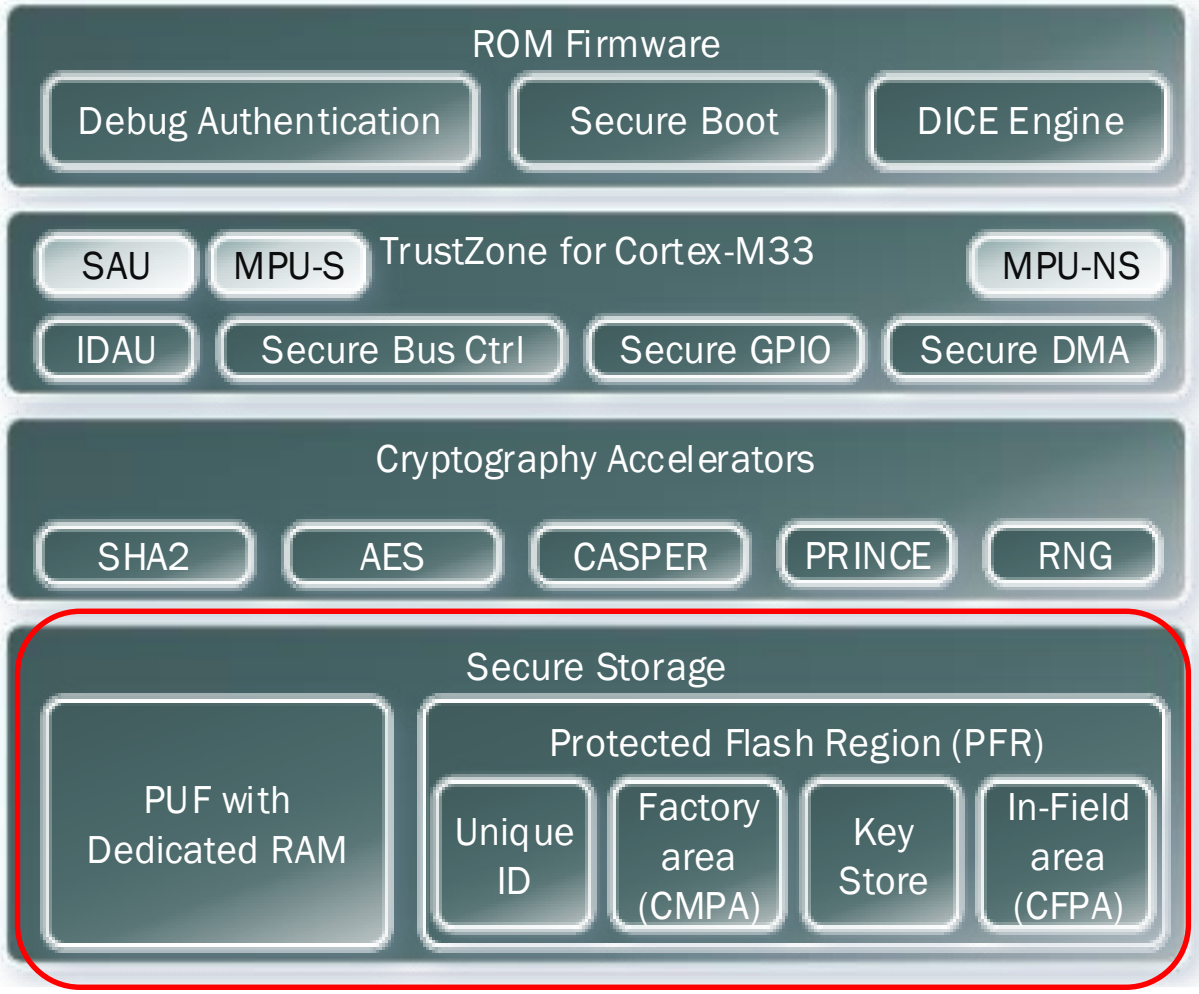
LPC55Sxx Security Sub-system

- **ROM supporting**
  - Secure Boot
  - Debug Authentication
  - DICE Engine
- **Trusted Execution Environment**
  - TrustZone
  - Security Attribution Unit (SAU)
  - Memory Protection Unit (MPU): Secure & Non-Secure
  - NXP IP
    - Defined Attribution Unit (using IDAU interface)
    - Secure Bus Control
    - Secure GPIO Controller
    - Secure DMA Controller
- **Cryptography Accelerators**
  - HashCrypt engine: AES and SHA
  - PRINCE on-the-fly flash encryption/decryption engine
  - CASPER: Asymmetric cryptography accelerator
  - Random Number Generator (RNG)



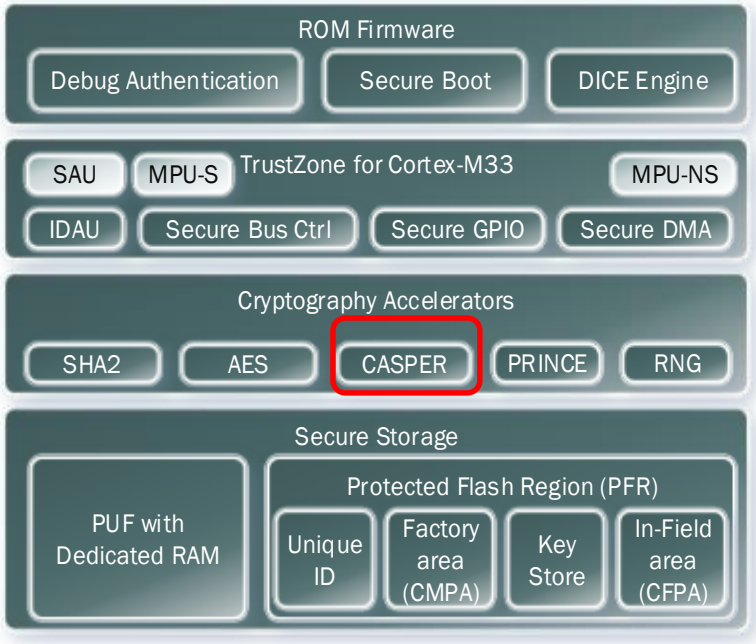
LPC55Sxx Security Sub-system (Cont…)

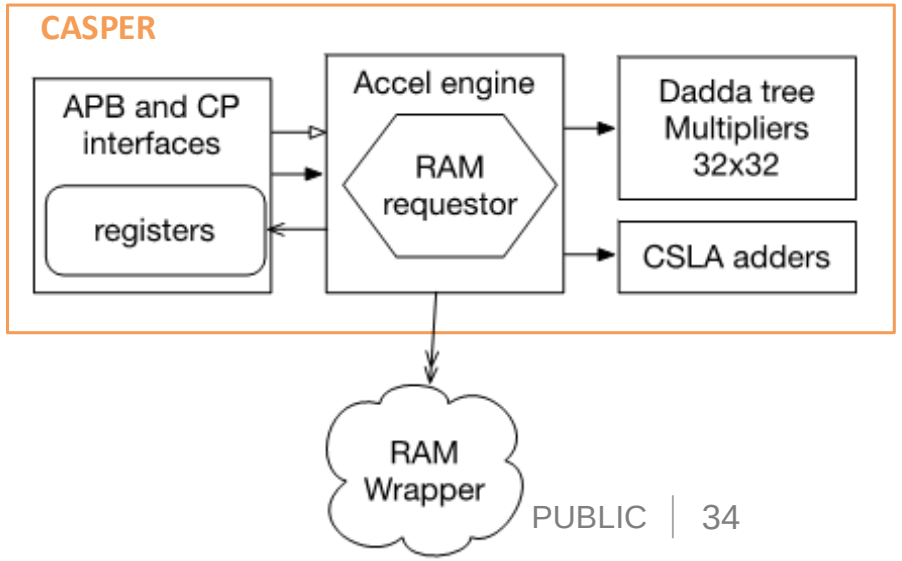
- Secure Storage
  - Physically Unclonable Function (PUF)
    - Device unique root key (256 bit strength)
    - Can store key sizes 64 bit to 4096 bit
  - Protected Flash Region
    - RFC4122 compliant 128-bit UUID per device
    - PUF Key Store
      - Activation code, PRINCE region key codes, FW update key encryption key, Unique Device Secret
    - Customer Factory Programable Area
      - Boot Configuration, RoT key table hash, Debug configuration, PRINCE configuration
    - Customer In-Field Programable Area
      - Monotonic counter, PRINCE IV codes



CASPER - Asymmetric Crypto Accelerator

- **Asymmetric cryptography challenge**
  - Require (very) large number mathematical operations
  - SW-only approach is painfully slow and power hungry
  - Algorithms continue to evolve
    - New ECC curves
    - OpenSSL baseline NIST curves: Elliptic Prime Curve 256 (EC_prime256v1), 384b
    - AWS adds 512b (EC_secp521r1)
  - Fixed HW-only solution is restrictive/obsolete
- **Coprocessor interface to Cortex-M33**
  - 64b data bus, offload CPU
- **Fast shared RAM access**
  - 2x32b RAMs allocated for CASPER, allowing 64b parallel access
- **A bank of Adder to allow MAC**
- **Two 32x32b multipliers**
- **Side channel protection**
- **Efficient for smaller size & better power**
- **SDK crypto lib**





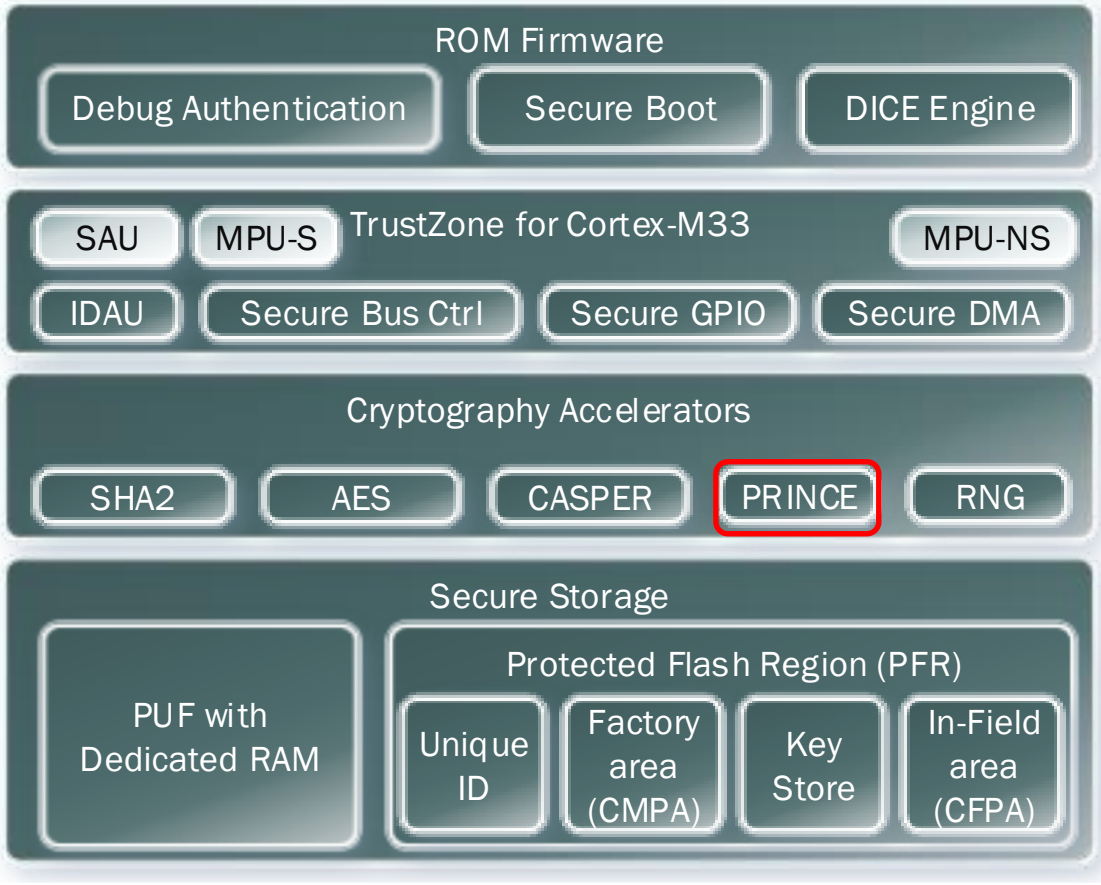
CASPER - Asymmetric Crypto Accelerator

Operation	System clock:150MHz IDE: IAR8.32, Optimizations: high-speed-no size constraints	SW only		CASPER accelerated		Improvement(times)	
		RAM	Flash	RAM	Flash	RAM	Flash
Signing	ECDSA-secp256r1(ms/sign)	136.43	333.33	76.92	142.86	1.77	2.33
Verification	ECDSA-secp256r1(ms/verify)	250.00	598.80	81.10	149.93	3.08	3.99
Key exchange	ECDHE-secp256r1(ms/handshake)	250.00	500.00	136.43	250.00	1.83	2.00
Key exchange	ECDH-secp256r1(ms/handshake)	136.43	300.30	71.43	130.38	1.91	2.30
Signing	RSA-1024(ms/private)	130.38	250.00	130.38	272.48	-	-
Verification	RSA-1024(ms/public)	4.24	8.90	1.31	1.81	3.24	4.93
Signing	RSA-2048(ms/private)	598.80	1000.00	598.80	1000.00	-	-
Verification	RSA-2048(ms/public)	15.54	31.92	4.14	5.03	3.76	6.35

Please refer to AN12445

PRINCE - Realtime Encrypt/Decrypt

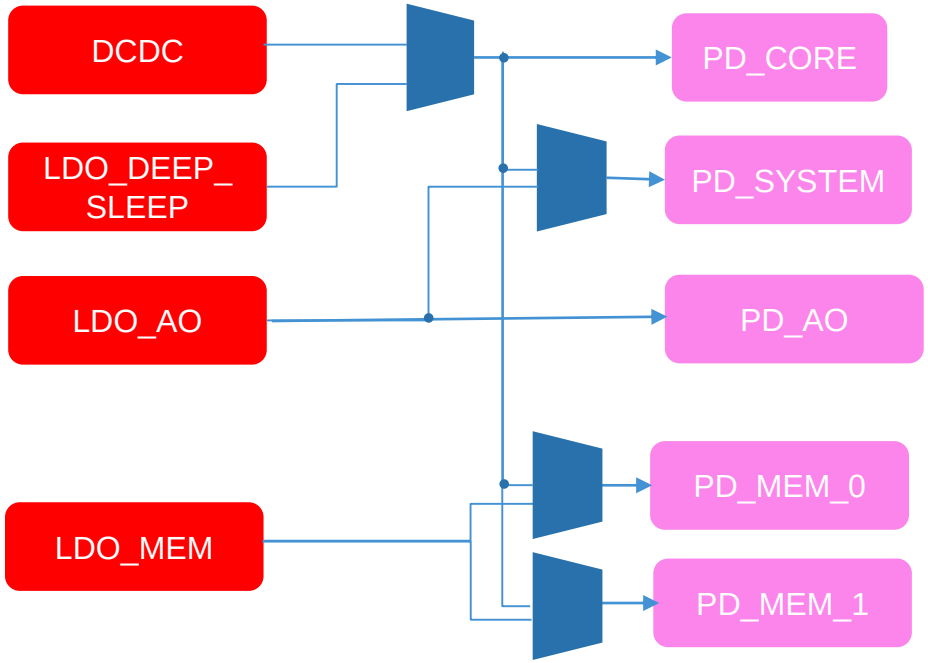
- **On-chip non-volatile storage used for important assets**
  - Secret keys
  - Proprietary SW from OEM and silicon manufacturer
  - Application Code
  - Other sensitive info
- Prone to malicious attacks
  - Clone the code
  - Tampering for illegally gaining trust, changing execution sequence/programming value
  - Stealing keys
- **Solution**
  - Encrypt the code stored in Flash w/o degrade the performance



Power Management

Power Management

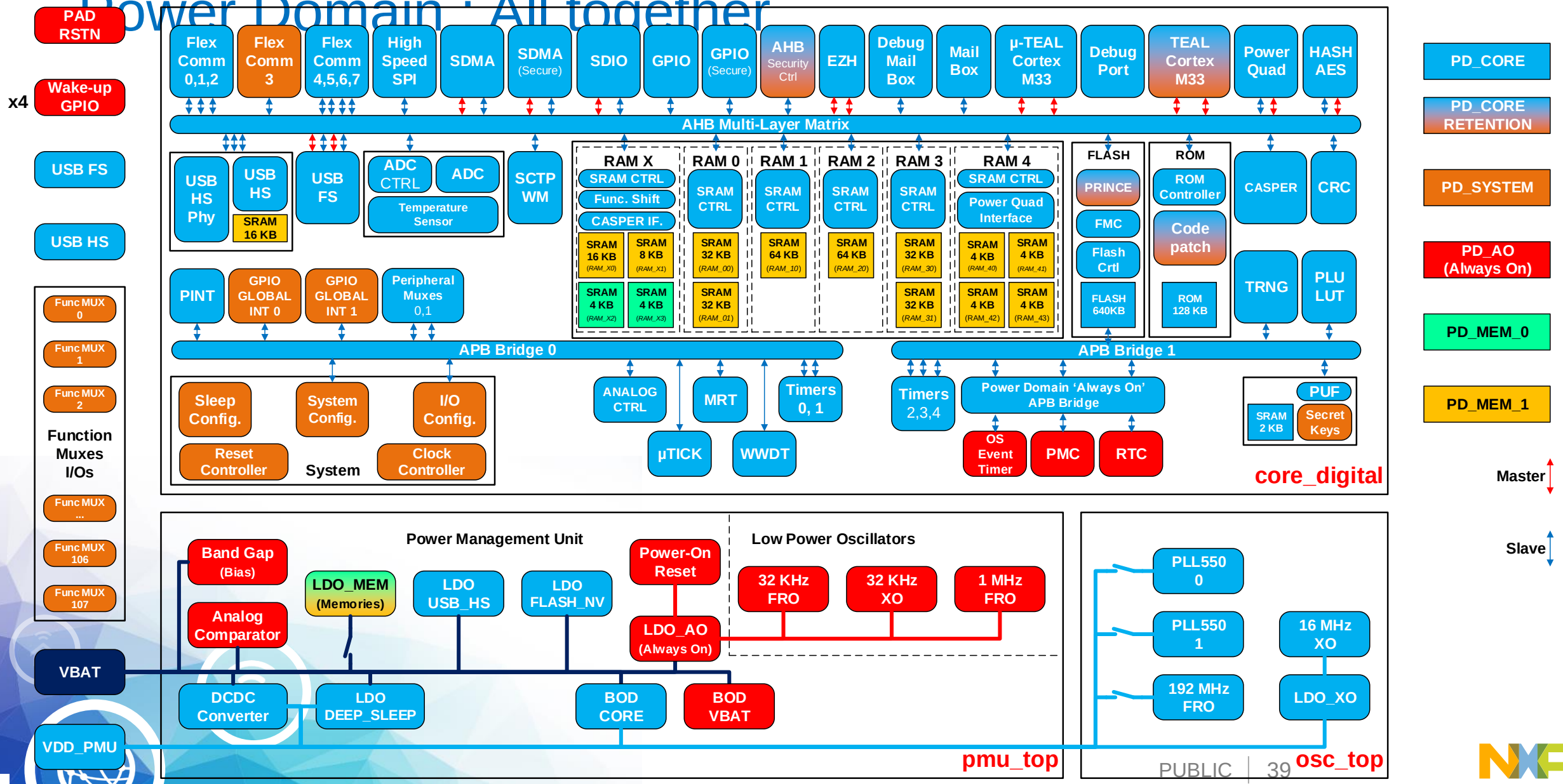
- 5 power domains, 7 on-chip regulators
  - All regulators can be supplied by single main external supply VBAT [1.8V – 3.6V]
- DCDC converter can be bypassed w/ external supply
- RBB with dynamic bias change to further reduce power
- Low dynamic power: ~40uA/MHz



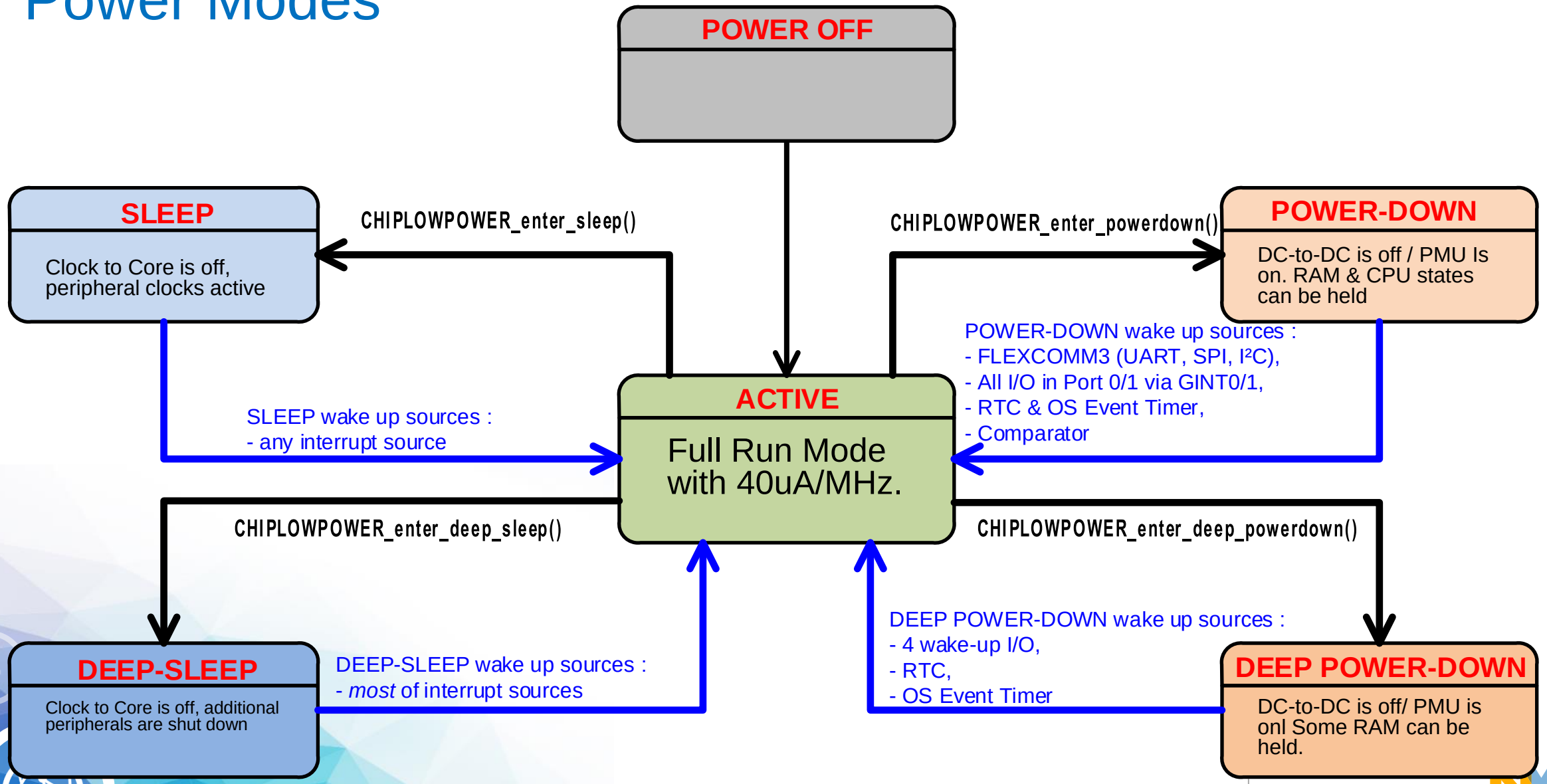
Power domain	Function Blocks
PD_CORE	Most of digital core logics (CPU0/1, AHB, Serial Peripherals, DMA, SDIO, etc)
PD_SYSTEM	Some critical system components (Clocks, Reset, Syscon, etc)
PD_AO	Always ON: PMC, RTC, etc
PD_MEM_0	Two 4KB SRAMs (RAMX_2/3)
PD_MEM_1	All other SRAMs

Regulators	Spec	Output
DCDC Buck Converter	0.950V – 1.200V	Main digital core logic
LDO_DEEP_SLEEP	0.9V – 1.075V	Deep-sleep
LDO_AO	0.75V – 1.220V	Always on digital logic
LDO_MEM	0.75V – 1.220V	SRAM in low power mode
LDO_USB_HS	1.8V – 2.0V	USB HS
LDO_FLASH_NV	1.8V – 2.0V	Flash macro

Power Domain : All together



Power Modes

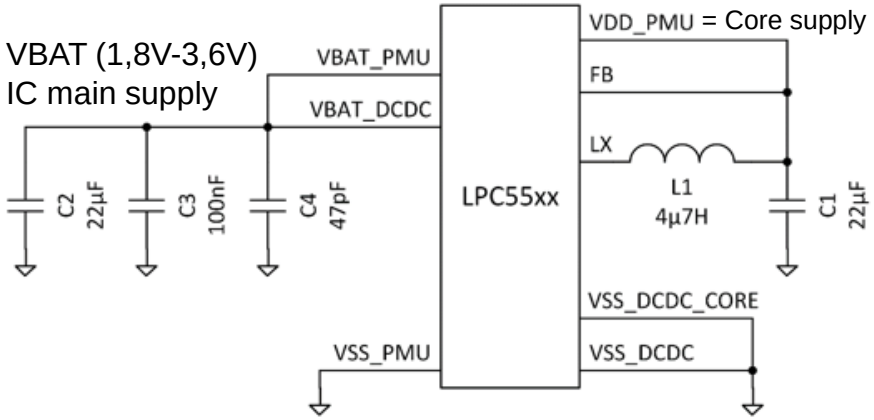

POWER OFF
SLEEP
Clock to Core is off, peripheral clocks active
CHIPLOWPOWER_enter_sleep()
CHIPLOWPOWER_enter_powerdown()
POWER-DOWN
DC-to-DC is off / PMU Is on. RAM & CPU states can be held
POWER-DOWN wake up sources :
- FLEXCOMM3 (UART, SPI, I²C),
- All I/O in Port 0/1 via GINT0/1,
- RTC & OS Event Timer,
- Comparator
ACTIVE
Full Run Mode with 40uA/MHz.
SLEEP wake up sources :
- any interrupt source
CHIPLOWPOWER_enter_deep_sleep()
CHIPLOWPOWER_enter_deep_powerdown()
DEEP POWER-DOWN wake up sources :
- 4 wake-up I/O,
- RTC,
- OS Event Timer
DEEP-SLEEP
Clock to Core is off, additional peripherals are shut down
DEEP-SLEEP wake up sources :
- *most* of interrupt sources
DEEP POWER-DOWN
DC-to-DC is off/ PMU is onl Some RAM can be held.

Power Modes

	Active	Sleep	Deep-Sleep	Power-Down	Deep Power-Down
CPU	ON	Stopped	Stopped	CPU0	OFF
SRAM	Configurable	Configurable	Configurable	Configurable	Configurable
Flash	Configurable	Configurable	OFF	OFF	OFF
ROM	ON	ON	OFF	OFF	OFF
Peripherals	Configurable	Configurable	Configurable	ACMP, Flexcomm3,Port0/1 PINT,RTC,OS Event Timer	RTC,OS Event Timer
Oscillators	Configurable	Configurable	Configurable	XTAL32K,FRO32K	XTAL32K,FRO32K

DCDC Converter

- Reduce power consumption and increase power efficiency
- Provide single supply to system
- Can be bypassed by providing core supply directly to VDD_PMU
  - 0.950V – 1.200V
- Startup time: ~100us (typical)
- Efficiency: >80% @load=50mA,
  >70% @load=4mA
- [AN12325]



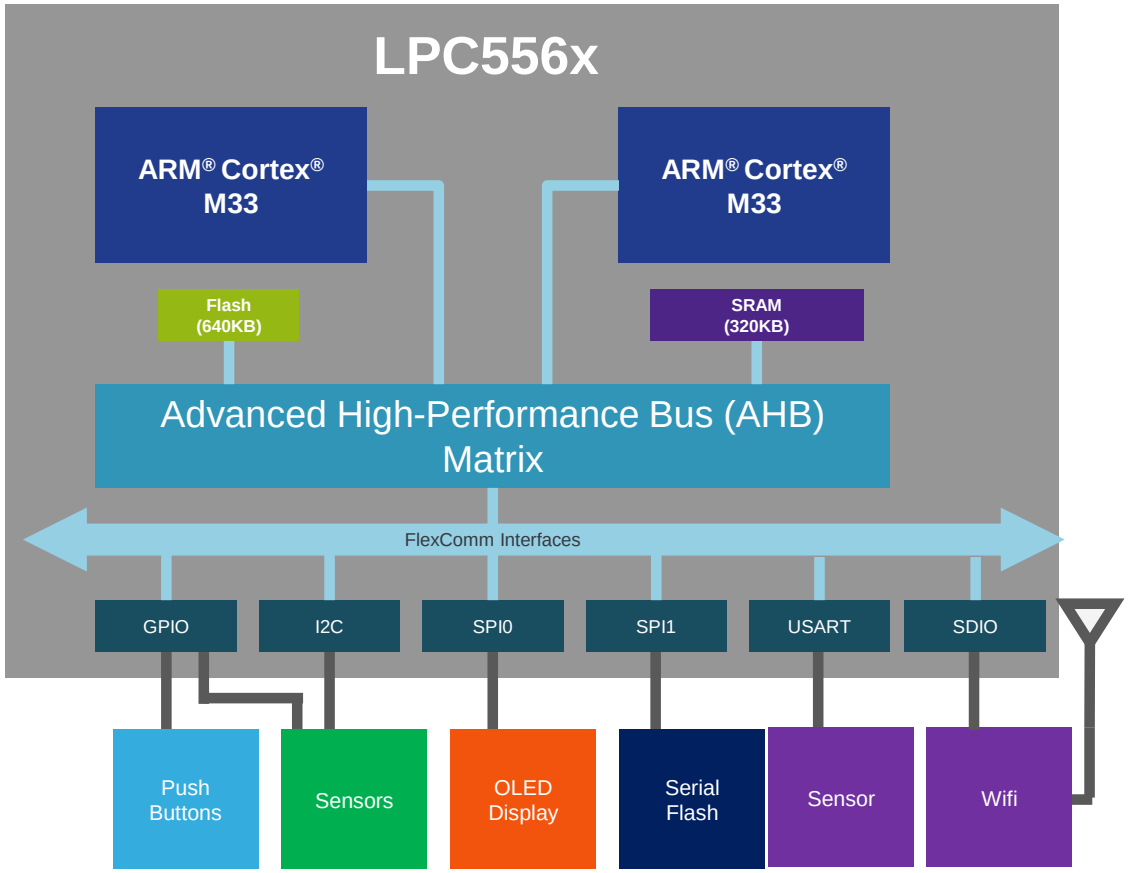
Part	Min	Typ	Max	Unit
C1	10	22 (X5R or X7R)	47	µF
C2	10	22 (X5R or X7R)	47	µF
C3	80	100 (X5R or X7R)	120	nF
C4	38.7	47 (COG)	56.2	pF
C5	80	100 (X5R or X7R)	120	nF
L1	3.87	4.7	10	µH

Pin Name	Pin number	
	HLQFP100	VBGA100
VBAT_DCDC	49	45
VBAT_DCDC_CORE	50	45
VBAT_PMU	51	46
VSS_DCDC	47	43
VSS_DCDC_CORE	46	42
VSS_PMU	-	47
LX	48	44
FB_VDD_PMU	45	41

System Infrastructure

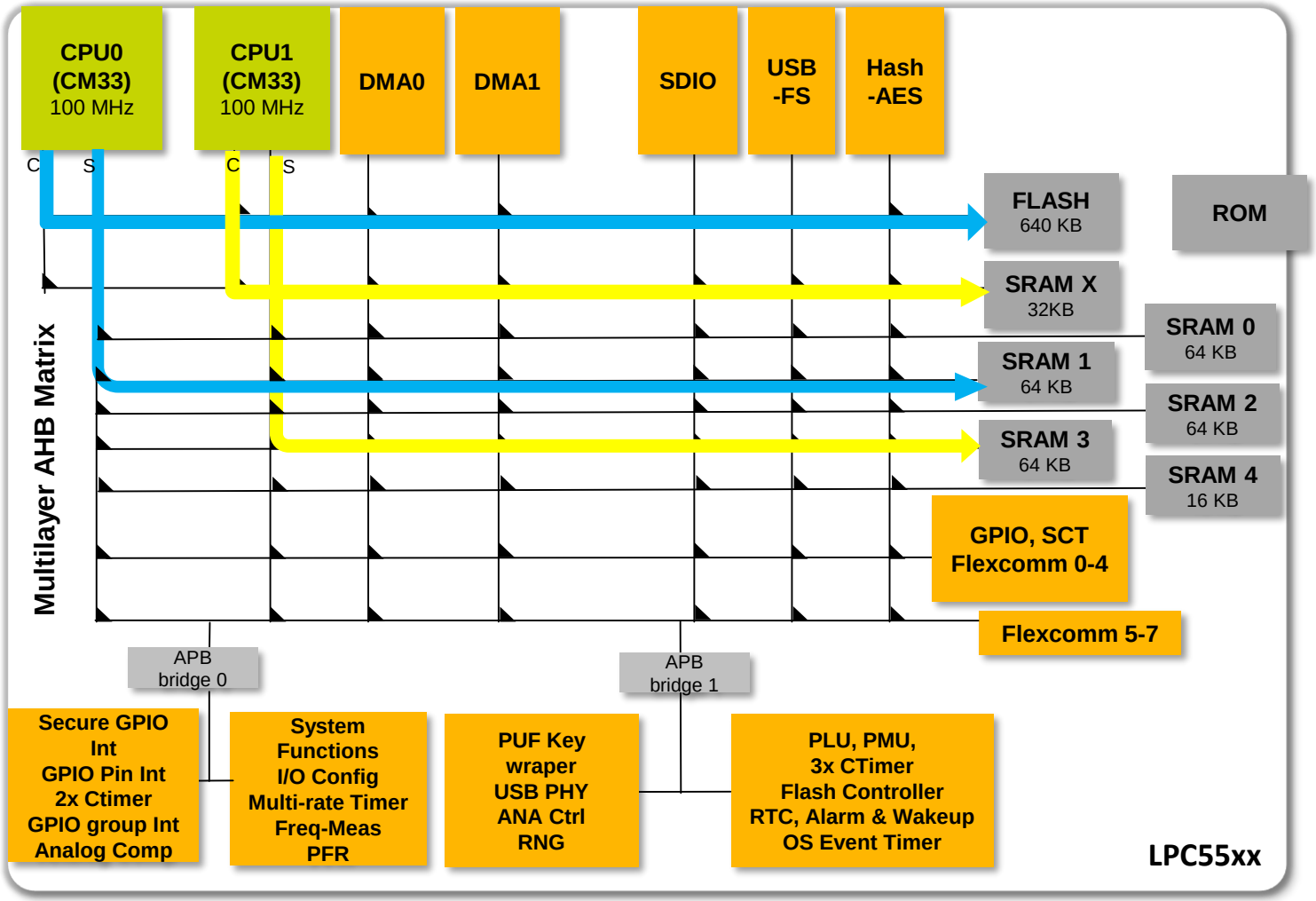
Asymmetric dual-core microcontroller architecture

- **Dual Core**
  - CPU0
    - Cortex-M33 with NVIC, FPU, MPU, DSP, ITM, SAU, TrustZone Security extension
    - Configured as primary CPU: Boots on Reset de-assertion, cannot be disabled
  - CPU1
    - Cortex-M33 with NVIC
    - Stays in reset until enabled by CPU0
  - Application partitioning
    - CPU1 can be leveraged for running system level tasks and the CPU0 can wake up to process data intensive tasks leveraging the co-processors
  - Mailbox used for multi-core communication and synchronization
  - Ease of software development
    - Software development teams can develop code for each core independently allowing for a faster time to market
- **Low Power Always-On Operation**
  - Provides low power always-on listening from analog and digital interfaces



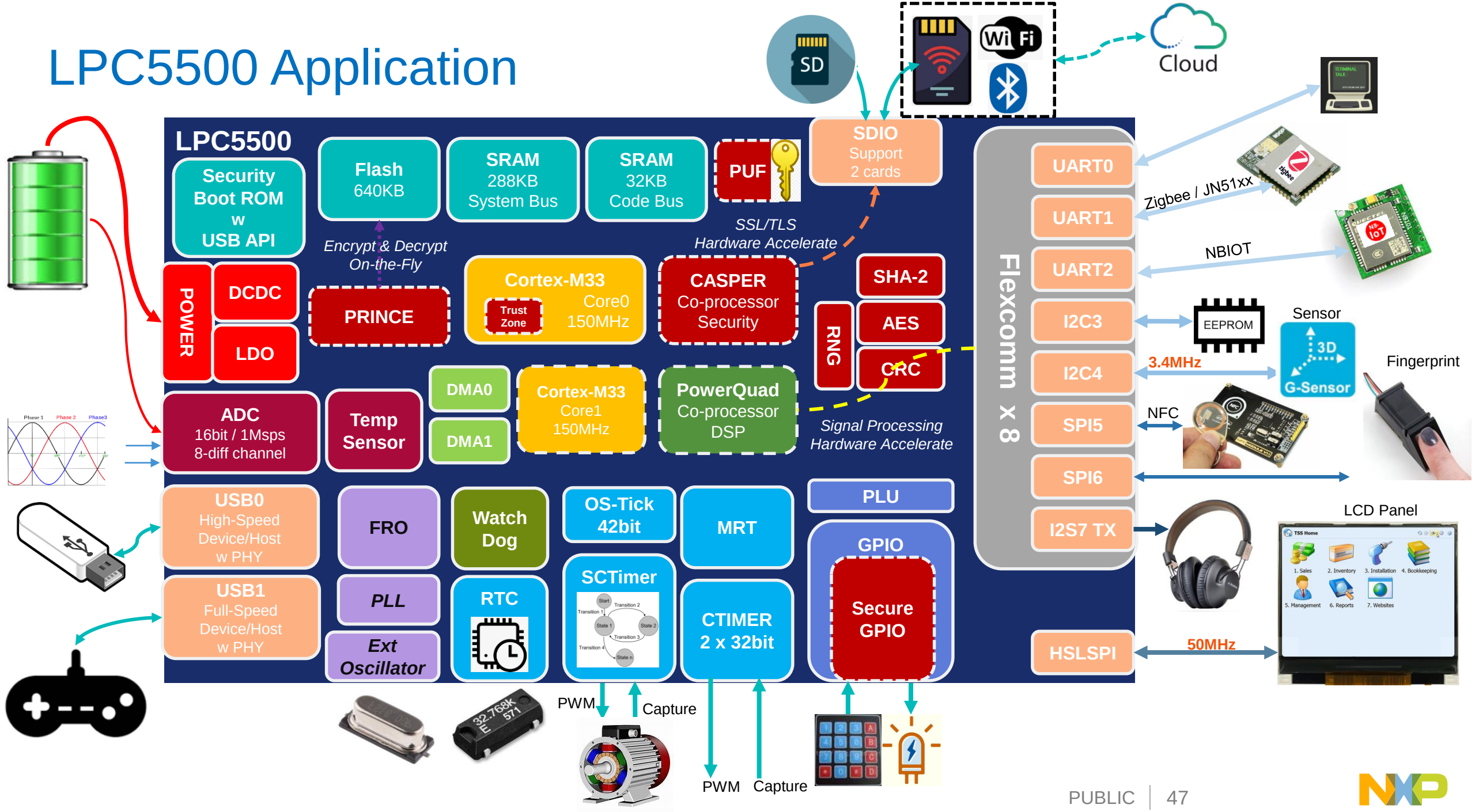
Bus Matrix configured for performance

- **Efficient Partitioning**
  - Allows both cores and DMAs to run at full speed with no contention
  - Memories and Peripherals are distributed on multiple slave ports and APB bridges allowing independently access from all bus masters
  - Contiguous system RAM
  - **Dual core: 7.55 CoreMark/MHz**
- **Programable Master priority**
- **Synchronous system clock**
  - Synchronous clock for all bus masters and slave AHB and APB register interfaces
  - Independent asynchronous peripheral interface clocks
  - Independent asynchronous timer/counter clocks



Enablement

LPC5500 Application



LPC5500 Tools

SW Tools

- **IDE**
  - IAR, KEIL, MCUXpresso IDE
- **SDK**
  - MCUXpresso SDK
  - MCUXpresso Config tools
    - pin/clock, TrustZone
    - Project cloner
- **Bootloader/FW update**
  - MCUboot – FW
  - Blhost – host
  - FlashMagic
- **Security**
  - ElftoSB GUI
  - SEC tool (Q1/2020)

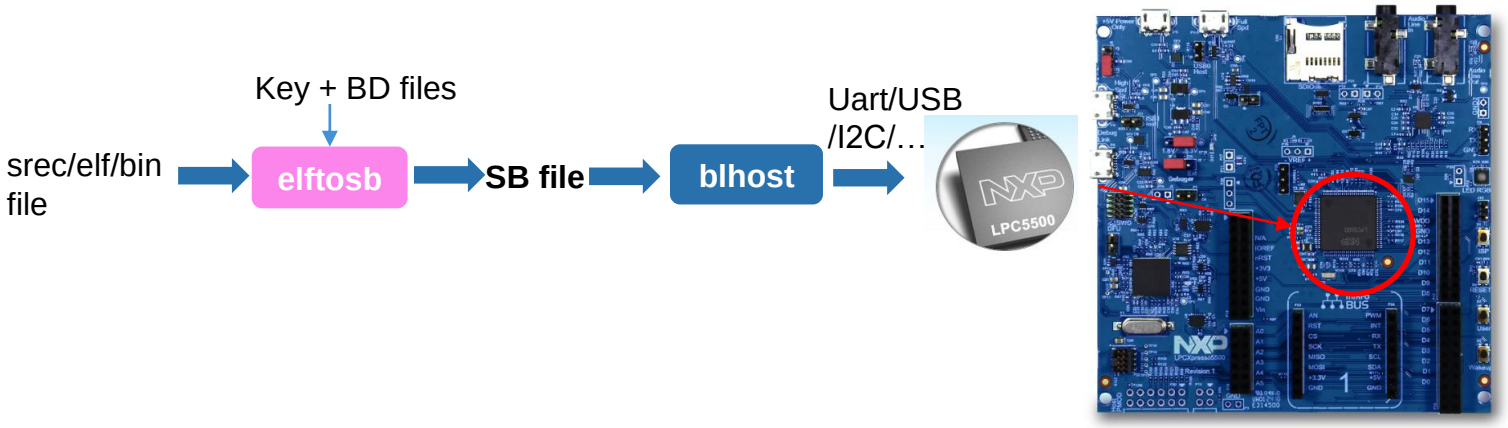
MCUXpresso SDK

MCUXpresso IDE

ARM KEIL Microcontroller Tools

IAR SYSTEMS

MCUXpresso Config Tools

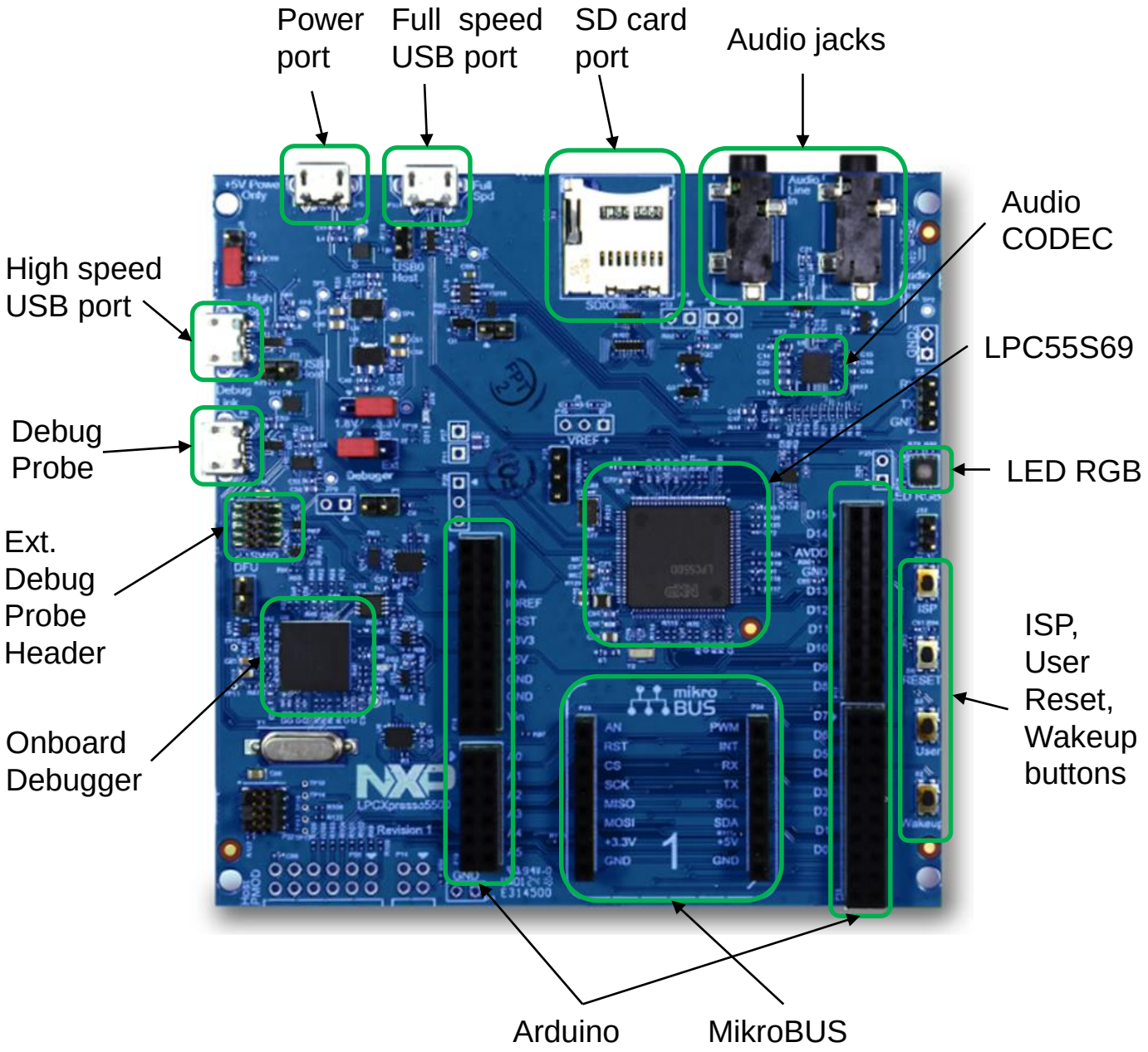


HW Tools

- **LPC55S69-EVK**

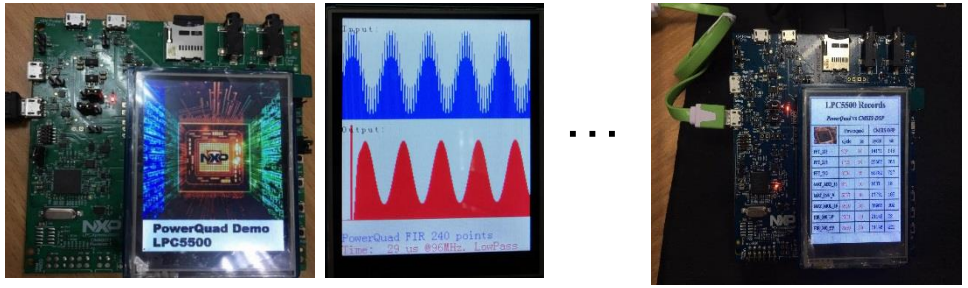
LPC55S69 EVK

- LPC55S69 LQFP100
  - World's First Arm® Cortex® -M33 based MCU Series, Leveraging 40nm Embedded Flash Technology
- Onboard debug probe
  - Support debugging without external debug probe
  - VCOM-based UART
- High/Full speed USB port
- Audio jacks IN and OUT
- On board audio CODEC
- SD card port
- LED RGB
- ISP, User, Reset, Wakeup buttons
- Expansion connectors
  - Arduino UNO R3 connector
  - MikroBUS connector
  - Other I/O headers



LPC5500 Demo

- LPC5500 High performance PowerQuad DSP Co-processor demonstration
  - Single cycle 4 x 32 bits single point floating MAC
  - HW accelerator for trigonometry/ Hypobolics/Matrix/Transform/Signal Processing/ Math computing
  - Faster than CMSIS-DSP by several or even dozen times
- LPC5500 Real-time PRINCE Encryption/Decryption demonstration
  - Real time flash encryption/decryption
  - Provide CPU + silicon + system level secure with other on-chip advanced secure technologies
- CMSIS-NN Machine Learning demonstration
  - Leverage CIFAR-10 model + CMSIS-NN to implement machine learning
  - Use single Coretex-M33, higher performance than CM4 by 15%+



PowerQuad demo

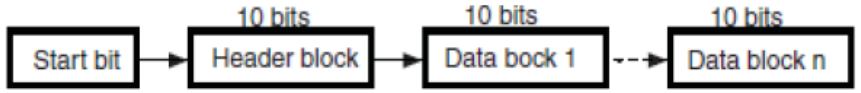
PRINCE demo

CMSIS-NN demo

HDMI-CEC implementation on LPC5500 series

HDMI CEC is a one-wire protocol aiming at reducing the remote controllers to control all the HDMI devices connected together through the HDMI cables serially.

- Customer: Sony
- Provide source code for implementing CEC physical layer
- Only using two GPIO + one SCT timer / Ctimer
- Hardware: LPC5500-EVK and HDMI cable
- Tested with Google Chromecast



Example of Header block:

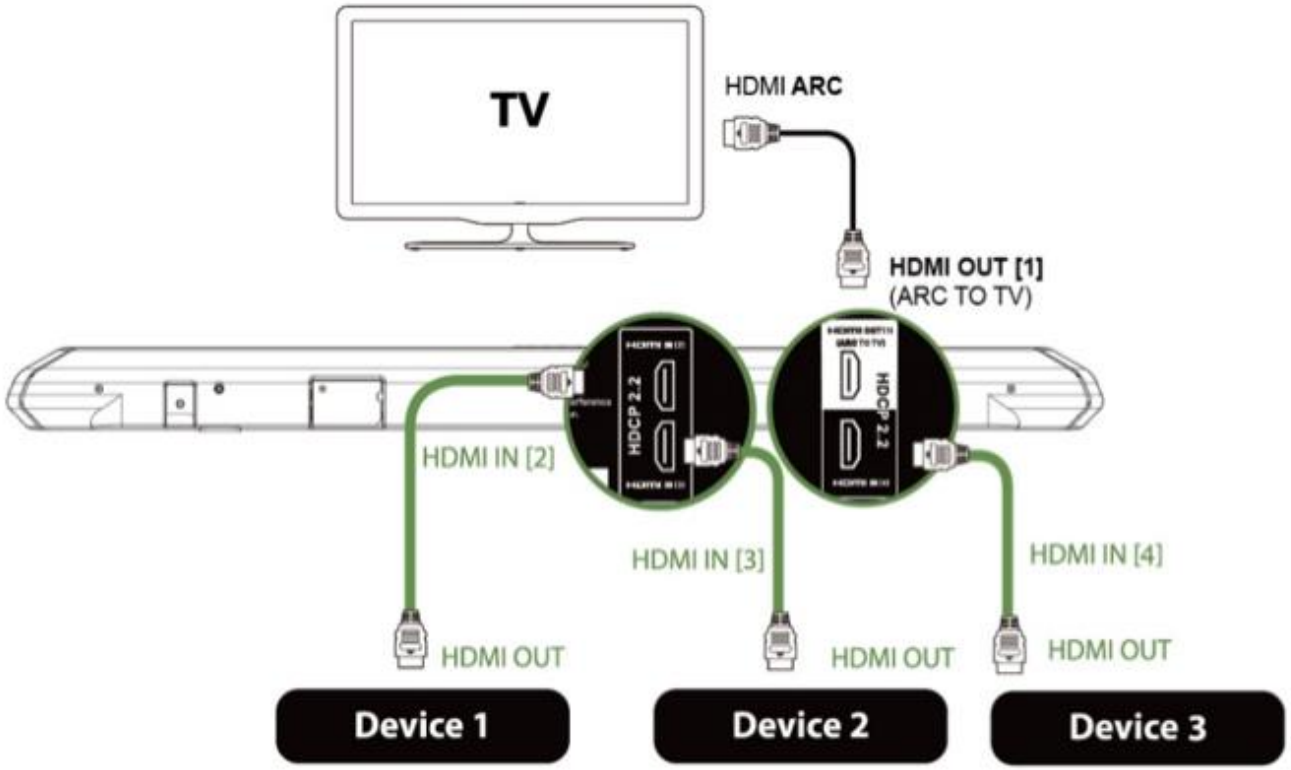
Initiator address = 0x6
Destination address = 0xD

Header block									
0	1	1	0	1	1	0	1	0	-
Initiator				Destination				EOM	ACK

Example of Data block:

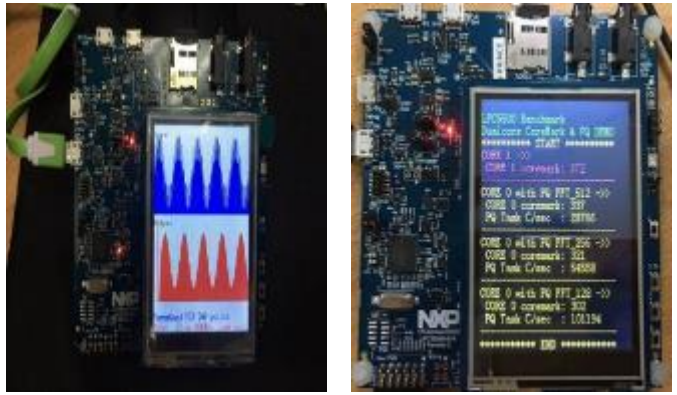
Data = 0xE5

Data block									
1	1	1	0	0	1	0	1	0	-
Data								EOM	ACK

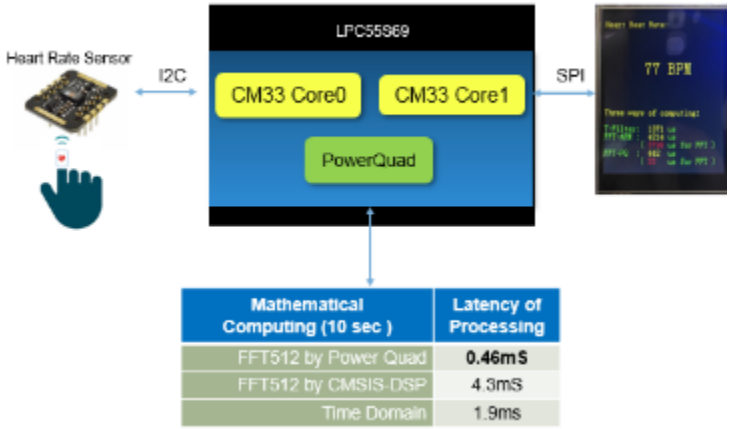


LPC5500 – PowerQuad Demos

- **Performance Benchmark Demo**
  - Single core w/ PQ demo
  - Dual core w/ PQ demo
  - IDD measurement
- **Biomedical Demos**
  - **Heart Rate Monitor**
    - Dual cores for different tasks
    - Three modes of computing heartbeat rate
  - **Sensor Fusion**
    - Fusion algorithm is implemented by PowerQuad of LPC55S69
    - 50% clock cycles less than pure software implementation in 9DOF algorithm
  - **KWS (Keyword Spotting)**
    - **Passcode Game**
      - TCN model by PQ
      - Audio data frame in 16ms, handled in each iteration of NN in ~3
      - Number recognition in real time
    - **Alexa demo**
      - TCN model by PQ
      - Accept the voice of “Alexa” and reject other word
      - LED indicator
      - Log in terminal

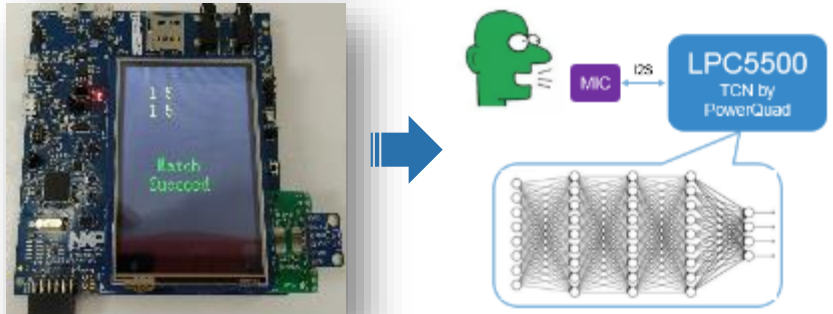


Performance Benchmark

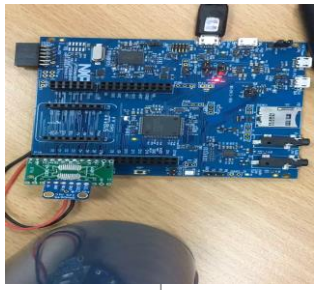


Heart Rate Monitor

Sensor Fusion



KWS Passcode Game



Alexa

LPC5500 for Fingerprint

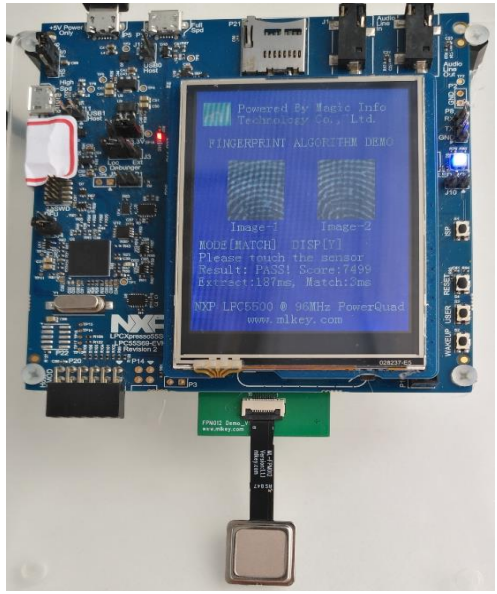
- BetterLife sensor based
  - FP lib provided by BetterLife, integrated by SE
  - Pure SW only, no PowerQuad
  - Faster recognition timing vs old version

BetterLife

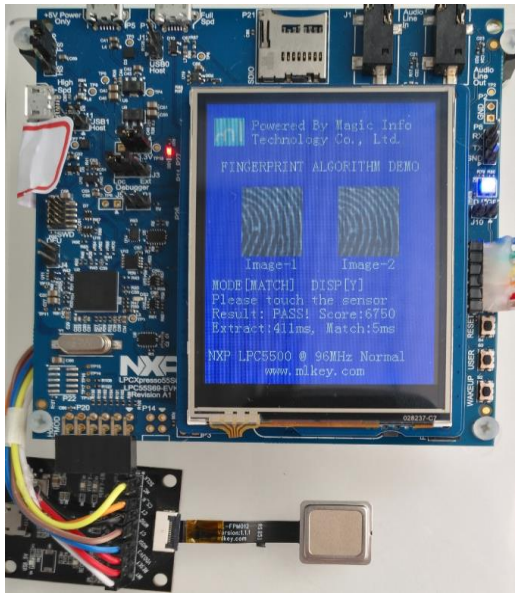
	LPC55S69 (ms)	LPC54101 (ms)
Enroll	300	455
Match (PASS)	48	75
Match (FAIL)	200	310
Extract	155	234

- Mlkey sensor based
  - Fully developed by Mlkey with PowerQuad and pure SW
  - Over 100% performance boost w/ PQ

	PowerQuad (ms)	SW only (ms)
Enroll	185	430
Match (PASS)	3	6
Match (FAIL)	5	25
Extract	180	406



Mlkey PQ



Mlkey SW only

LPC5500 Technical Content

Product

1. **User Manual**
2. **Data Sheet**
3. **Errata**
4. **Fact sheet**

AN/Video

1. TrustZone using CMSIS examples (FreeRTOS and bare metal),
2. **Computing FFT with PowerQuad and CMSIS-DSP on LPC5500**
3. **AN12282 - Digital Signal Processing for NXP LPC5500 Using PowerQuad**
4. **AN12387 - Running Coremark Benchmark with Dual CM33 Cores and PowerQuad**
5. **AN12383 - Computing FFT with PowerQuad and CMSIS-DSP**
6. SD/MMC demo with SPI display and encrypted using PRINCE
7. **LPC55Sxx PRINCE Real-time Data Encryption**
8. Low Power modes
9. **AN12327 - Firmware Update Using Secondary Bootloader**
10. **AN12283 - Secure Boot** with encrypted image/signed image
11. **AN12358 - Dual-Core Debug in MCUXpresso**
12. **AN12335 - Dual Core Communication**
13. **AN12325 - Using the DCDC Feature**
14. **AN12326 - Secure GPIO and Usage**
15. AN12458 - USB to Virtual COM on LPC54018 and LPC5500
16. AN12445 - Asymmetric Cryptographic Accelerator CASPER
17. AN12581 - 2-layer PCB Layer Design Guide for VFBGA98 Package
18. AN12456 - Shell Solution on NXP LPC5500 Series
19. AN12324 - LPC55Sxx Usage of the PUF and Hash Crypt to AES Coding
20. TN00065 – Crystal-less USB solution
21. AN12728 – CANFD
22. AN12278 – Security solution for IoT
23. AN12732 – HDMI-CEC solution
24. Secure debug authentication, in plan
25. 16b fast ADC, in plan
26. Security features [Video, Oct 18]
27. Enabling secure, NB-IoT end nodes with MCUXpresso enablement and PSA-certified MCU
28. **Enabling Next-Gen IoT Applications With Secure-enabled NXP MCUs with TrustZone®-M Technology**
29. CANopen and NXP MCU
30. **Secure Provisioning and Programming Using Embedded Trust and the Security-enabled LPC55S6x MCU**
31. MCUXpresso SDK Overview
32. IDE & Configuration Tools Overview
33. Security Tools Overview, in plan

Training

1. LPC5500 Architecture Introduction
2. PowerQuad DSP
3. TrustZone
4. Secure boot
5. Low Power Mode
6. Performance benchmarking
7. Security features: PUF, PRINCE, …
8. …

SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com

NXP, the NXP logo, and NXP secure connections for a smarter world are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2019 NXP B.V.

TECHNOLOGY
DAYS

www.nxp.com

NXP, the NXP logo, and NXP secure connections for a smarter world are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2019 NXP B.V.