

# MSPM0 AES module introduction

— MSPM0 peripheral training series

Presented by Cash Hao

# MCU level overview

## —MSPM0Lxx series

### MSPM0L13x3/4/5/6

1.62 - 3.6V  
-40 to 125 C

<b>CPU</b> <b>ARM Cortex-M0+</b> <b>32 MHz</b>	<b>Power &amp; Clocking</b>	<b>Precision Analog</b>
NVIC / 3-ch DMA	POR / BOR / SVS	12-bit SAR ADC 1Msps (1)
	Internal LF 32kHz (5%)	ULP/HS Comparator (1)
	Internal HF 4-32MHz (1%)	8-bit reference DAC (1)
<b>On-chip Memory</b>	<b>Communication</b>	Zero-drift chopper op-amps (2)
8, 16, 32 or 64 kB flash	UART w/ LIN (1)	General purpose amp (1)
2 or 4 kB SRAM	UART (1)	Internal ADC reference (2.5%)
<b>Data Integrity &amp; Security</b>	SPI (1)	Temperature sensor
CRC accelerator (16 and 32 bit)	I2C (2) w/ FastMode+	<b>Timers</b>
<b>Programming &amp; Debug</b>	<b>IO</b>	General purpose 16-bit 2 CC (4)
ARM SWD interface	Up to 28 GPIO	Windowed watchdog
ROM UART & I2C BSL	Up to 2 low Ib OPA inputs	

Leaded packages: SOT-16, VSSOP-20/28  
No-lead packages: WQFN-16, VQFN-24/32

*32 MHz MCU with up to 64kB flash, 32 pins, 12-bit ADC, dual zero-drift OPA/PGA, COMP*

## —MSPM0Gxx series

### MSPM0G350x/310x/150x/110x

1.62 - 3.6V  
-40 to 125 C

<b>CPU</b> <b>Arm Cortex-M0+</b> <b>80 MHz</b>	<b>Power &amp; Clocking</b>	<b>Precision Analog</b>
NVIC / MPU / 7-ch DMA	POR / BOR / SVS	12-bit ADC 4Msps (9-ch)
<b>Accelerators</b>	External LF 32kHz XTAL	12-bit ADC 4Msps (8-ch)
Math (DIV, SQRT, TRIG, MAC)	External HF 4-48MHz XTAL	Comparators w/ 8-bit DACs (3)
<b>On-chip Memory</b>	Internal LF 32kHz (3%)	12-bit 1Msps buffered DAC (1)
32, 64, or 128 kB flash [ECC]	Internal HF 4-32MHz (1%)	Zero-drift chopper op-amps (2)
16 or 32 kB SRAM [ECC]	PLL (up to 80 MHz)	Internal reference (1.5%)
<b>Data Integrity &amp; Security</b>	<b>Communication</b>	General purpose amp (1)
CRC accelerator (16 and 32 bit)	UART w/ LIN (1)	Temperature sensor
AES256 accelerator + TRNG	UART (3)	<b>Timers</b>
<b>Programming &amp; Debug</b>	SPI (2)	Advanced control 16-bit 4 CC (1)
ARM SWD interface	I2C (2) w/ FastMode+	Advanced control 16-bit 2 CC (1)
UART & I2C bootloader	CAN-FD (1)	General purpose 32-bit 2 CC (1)
	<b>IO</b>	General purpose 16-bit 2 CC (2)
	Up to 60 GPIO	Low power 16-bit 2 CC (2)
		Windowed watchdog (2)
		Real-time clock (1)

Leaded packages: VSSOP-20/28, LQFP-48/64  
No-lead packages: VQFN-24/32/48, nFBGA-64, WCSP-28

*80 MHz MCU with up to 128kB flash, 64 pins, advanced analog, AES/TRNG, CAN-FD*

# MSPM0G350x AES module introduction

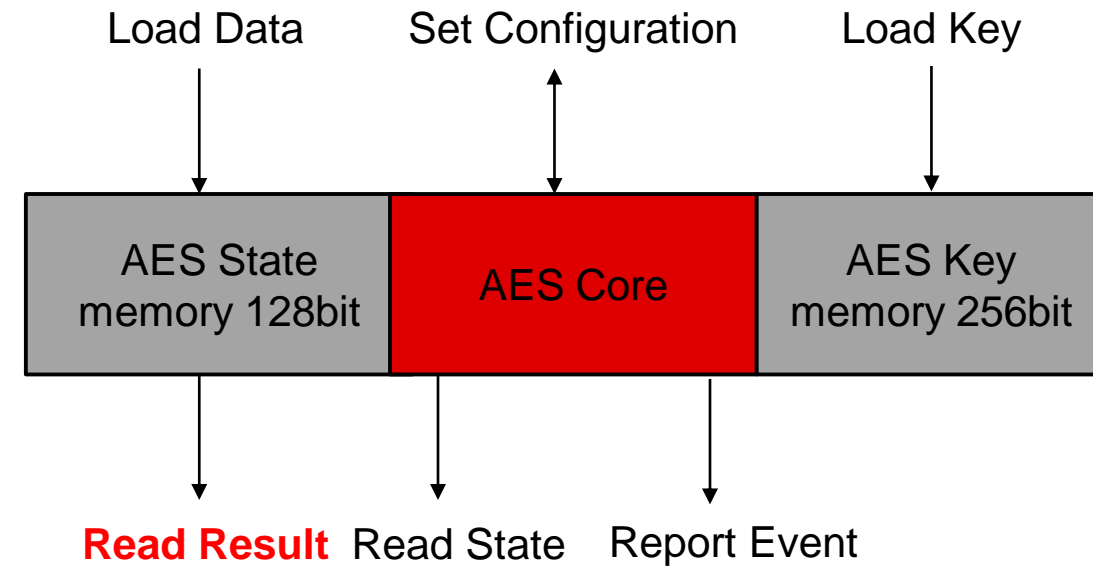
## Key Features

- FIPS PUB 197 advanced encryption standard
- AES 128-bit block encryption and decryption
- On-the-fly key expansion for encryption and decryption
- Offline key generation for decryption
- 8-bit byte or 32-bit word access to provide key data, input data, and output data

AES Key Length	Encryption			Decryption		
	Cycles	Time(32 MHz)	Time(80 MHz)	Cycles	Time(32 MHz)	Time(80 MHz)
128bit	168	5.25us	2.10us	168	5.25us	2.10us
256bit	234	7.31us	2.93us	234	7.31us	2.93us

## Key Differences between G and L MCUs

- MSPM0G350x MCUs have 1 AES module



# AES module quick start

## Academy

[AES introduction lab](#)

## Driverlib Examples

MSPM0G350x:

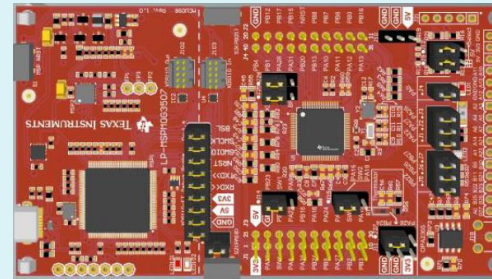
- aes\_cbc\_256\_enc\_dec
- aes\_ofb\_128\_encrypt

## Related Links

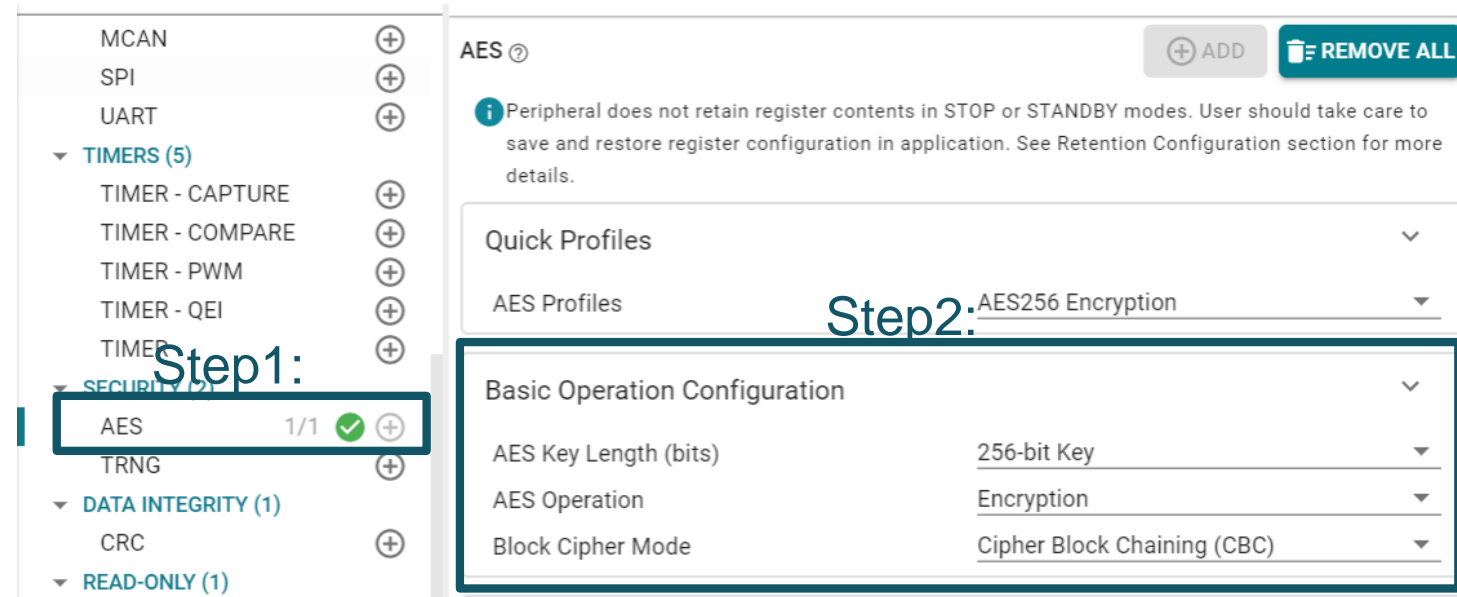
- [MSPM0 online resource](#)
- [MSPM0 Quick start guide](#)
- [MSPM0 Sysconfig user's guide](#)
  
- [MSPM0G350x datasheet](#)
- [MSPM0Gxx technical reference manual](#)

## Launchpad

LP-MSPM0G3507



## Sysconfig Entrance for AES Setting



MCAN (+)

SPI (+)

UART (+)

▼ TIMERS (5)

TIMER - CAPTURE (+)

TIMER - COMPARE (+)

TIMER - PWM (+)

TIMER - QEI (+)

TIMER (+)

▼ SECURITY (2)

**AES** 1/1 ✓ (+)

TRNG (+)

▼ DATA INTEGRITY (1)

CRC (+)

▼ READ-ONLY (1)

AES ⓘ

⊕ ADD REMOVE ALL

ⓘ Peripheral does not retain register contents in STOP or STANDBY modes. User should take care to save and restore register configuration in application. See Retention Configuration section for more details.

Quick Profiles ▼

AES Profiles

**Step2:** AES256 Encryption ▼

Basic Operation Configuration ▼

AES Key Length (bits) 256-bit Key ▼

AES Operation Encryption ▼

Block Cipher Mode Cipher Block Chaining (CBC) ▼

# To find more MSPM0 training series, please visit:

- [Ti.com.cn](http://ti.com.cn)
- [WeChat \(德州仪器公众号\)](#)
- [Bilibili](#)
- [21IC](#)