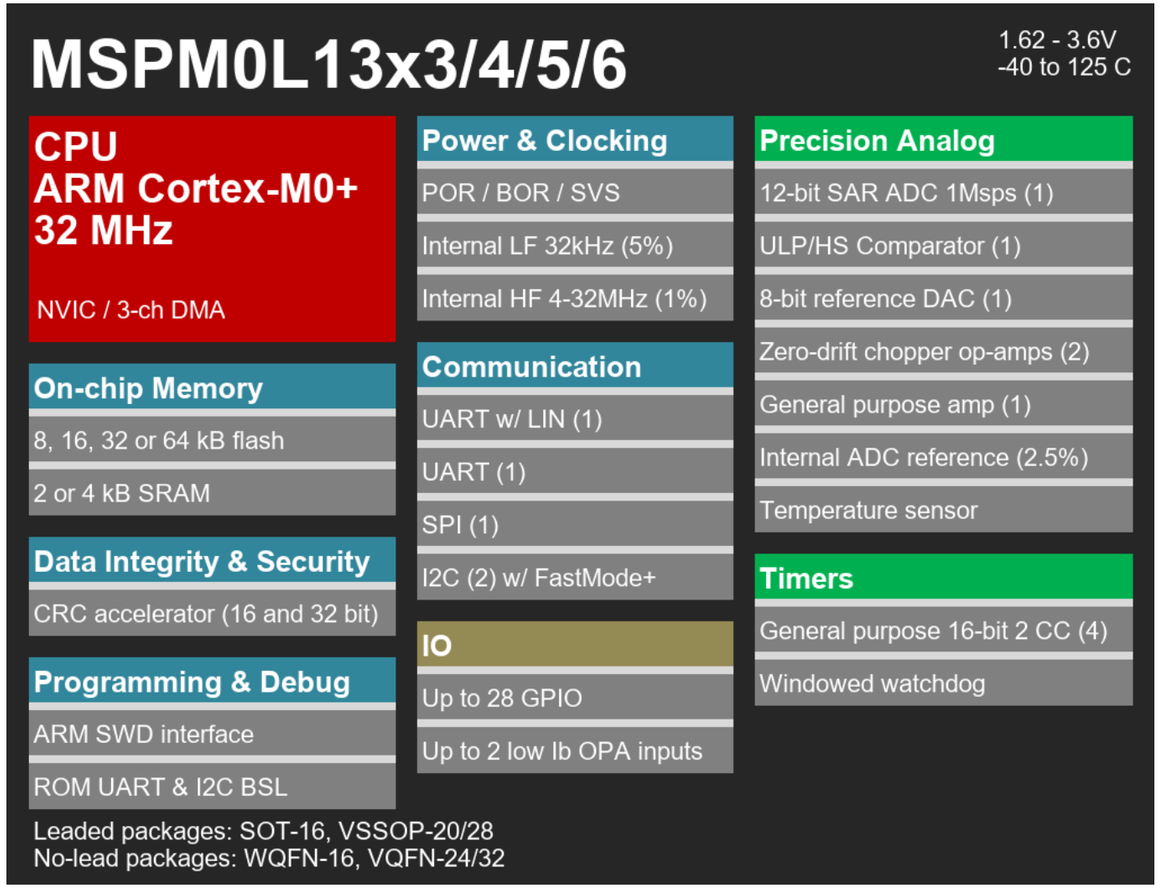
MSPM0 AES module introduction

—— MSPM0 peripheral training series

Presented by Cash Hao

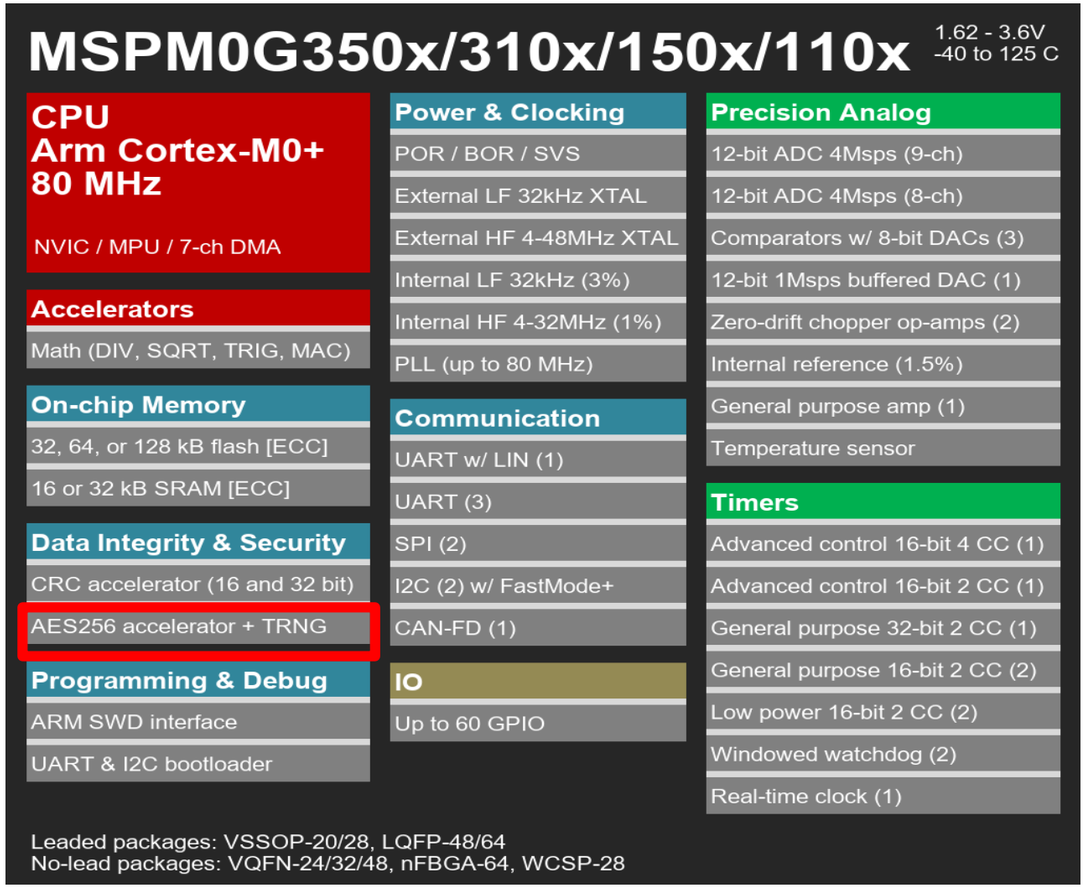
MCU level overview

——MSPM0Lxx series



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

——MSPM0Gxx series



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

MSPM0G350x AES module introduction

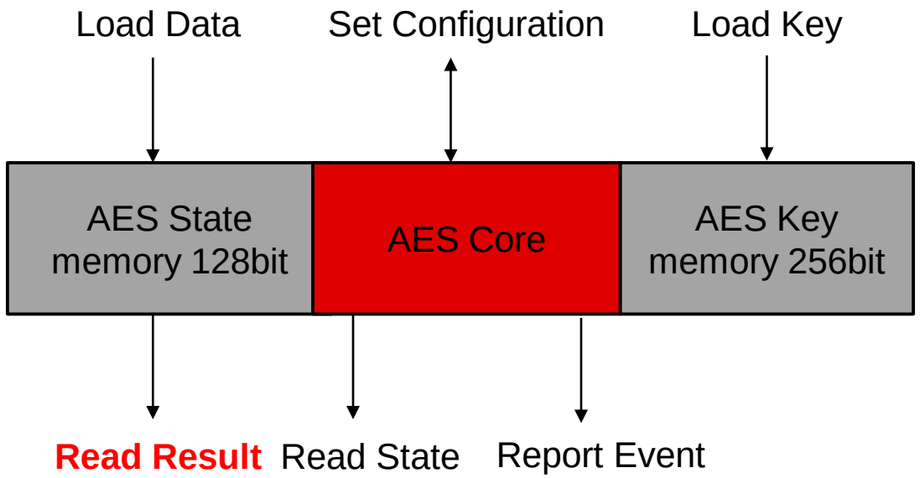
Key Features

- 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

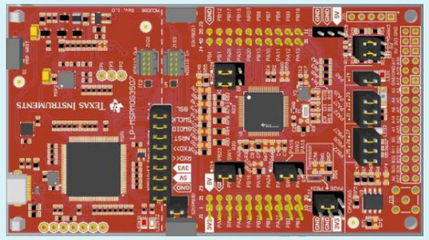
Related Links

MSPM0 online resource
MSPM0 Quick start guide
MSPM0 Sysconfig user's guide

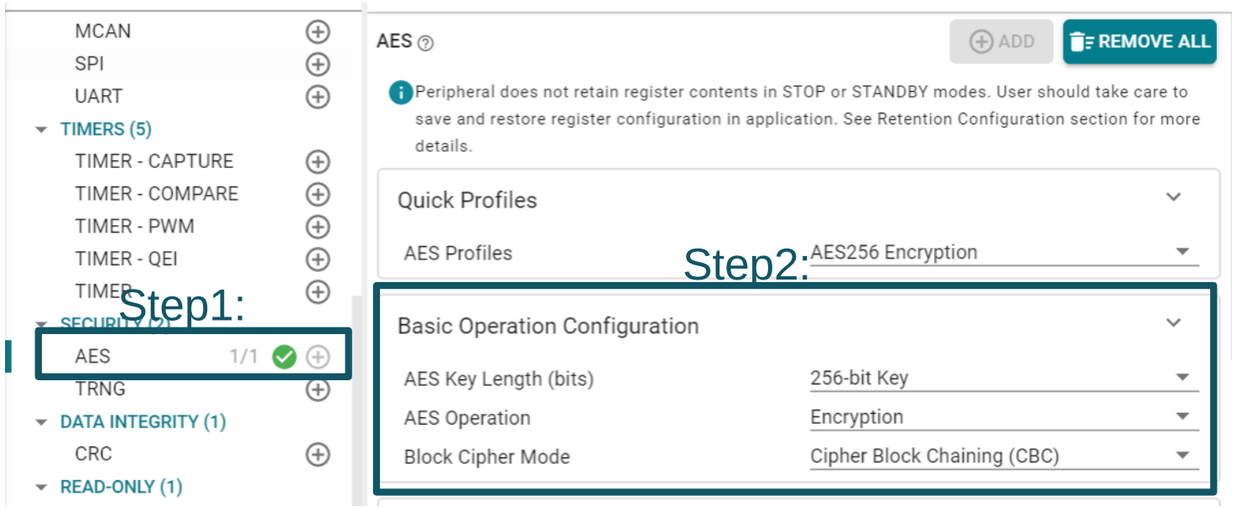
MSPM0G350x datasheet
MSPM0Gxx technical reference manual

Launchpad

LP-MSPM0G3507



Sysconfig Entrance for AES Setting



To find more MSPM0 training series, please visit:

- TI.com.cn
- WeChat (德州仪器公众号)
- Bilibili
- 21IC