NuMicro® Family

Based on Arm® Cortex®-M23

M2354 Series

Product Brief

For additional information or questions, please contact Nuvoton Technology Corporation.

www.nuvoton.com

1 GENERAL DESCRIPTION

The NuMicro® M2354 Series is a TrustZone® for Armv8-M architecture empowered microcontroller series focusing on IoT Security based on Arm® Cortex®-M23 CPU core technology. It runs up to 96 MHz with 1024 Kbytes embedded Flash memory and 256 Kbytes SRAM, supporting Flash in dual-bank mode, secure firmware OTA (Over-The-Air) update, ultra-low power consumption in normal run with 89.3 uA/MHz in LDO mode, 39.6 uA/MHz in DC-DC mode and an 8x40 COM/SEG LCD driver inside. Besides the fundamental microcontroller security features, it further enhances the chip-level security in covering side-channel attacks mitigation to crypto hardware engine, fault injection mitigation for operating voltage and clock as well as active shield to cryptographic key storage. The series supports power supply voltage from 1.7V ~ 3.6V in operating temperature range from -40°C to +105°C, and is equipped with both LDO and DC-DC power supply functionalities. The M2354 Series is quite competitive for those devices that need more secure, fast computing and low power in the IoT market.

The one of major challenges for IoT devices that are connected to cloud services or other devices by network communication is security, so the IoT devices must meet some security requirements to protect firmware, software and secure assets from being stolen or modified by an attacker. "**Execution**", "**Storage**", and "**Connectivity**" are the three important security targets for IoT devices.

The TrustZone® technology based on Armv8-M architecture is a System-on-Chip (SoC) and CPU system-wide approach to microcontroller security. The whole system isolates secure and normal worlds to avoid the trusted assets being accessed by a non-secure process. In addition to the firmware-level security, the M2354 series is also equipped with rich functions to improve system security. The Secure Bootloader supports trusted system-boot feature which can protect certificated firmware from being replaced with malware possibly in the upgrade processing and taking control of system resource finally. The hardware crypto accelerators, including AES, ECC and RSA, support encryption and decryption operations to offload the main processor's computing power and ensure data transmission in secure.

The M2354 series also enhances firmware update security requirement with monotonic version counter. The firmware cannot be rollback to older one which has lower security protection. Furthermore, there is a secure crypto keys storage protected by the chip-level active shield function to physical intrusion. The series addresses the physical attack protection and system security certification for Arm® PSA Certified™ Level 2 even for PSA Certified™ Level 3.

Other than security, low power is also vital for IoT applications. The M2354 series supports 4 core power levels with both LDO and DC-DC power supply mechanism. Except normal run mode, the series also provides idle run mode with power consumption 31.5 µA/MHz in LDO mode and 14.3 µA/MHz in DC-DC mode. The current consumption of Deep Power-Down mode without V_{BAT} is less than 0.1 µA.

The M2354 series is equipped with plenty of peripherals such as Timers, Watchdog Timers, RTC, PDMA, UART, Universal Serial Control Interface (USCI), SPI/ I²S, I2C, GPIOs, makes it highly suitable for connecting comprehensive external modules. The M2354 integrates high performance analog front-end circuit blocks, such as 16 channels of 12-bit 6 MSPS ADC, temperature sensor, low voltage reset (LVR) and brown-out detector (BOD) to enhance product performance, reduce external components and form factor simultaneously. Moreover, it supports up to 8x40 COM/SEG for segment LCD display needed such as metering devices.
The M2354 series provides LQFP48 (7mm x 7mm), LQFP64 (7mm x 7mm) and LQFP128 (14mm x 14mm).

Target Applications

- IoT Devices with Secure Connection
- Collaborative Secure Software Development
- Secure Fingerprint Lock
- Smart Home Appliances
- Secure Wireless Connectivity Module
- Auto Meter Reading (AMR)
- Portable Wireless Data Collector
- Digital Currency Authentication

- Smart City Facilities
- Wireless Sensor Node Device (WSND)

2 FEATURES

- **System and operating characteristics**
  - Voltage range: 1.7 V to 3.6 V
  - Temperature range: -40°C to +105°C
  - ESD HBM 2KV, EFT 4.4KV
  - 4 selectable core power voltage levels: PL0 (1.26 V, 96 MHz), PL1 (1.2V, 84 MHz), PL2 (1.0 V, 48 MHz), PL3 (0.9V, 12 MHz) in run and idle mode
  - DCDC and LDO voltage regulator modes
  - 5V tolerant I/O except analog pin
  - Up to 6 I/O pins supporting VAI with supply V_{DDIO} from 1.7 to 3.6 V
- **Core**
  - Up to 96 MHz Arm® Cortex®-M23 core delivering 0.95 DMIPS per MHz
  - 32-bit Single-cycle hardware multiplier and 32-bit 17-cycle hardware divider
  - 8 Memory Protection Unit (MPU) memory regions
  - 8 Security Attribution Unit (SAU) memory regions
  - Supports Armv8-M TrustZone®
- **Memories**
  - **1024 KB** of dual bank Flash memory with 4 KB one-way cache and zero-wait state when continuous address read
  - Dual bank Flash memory allows read-while-write programming and address remap function for fast firmware update purpose
  - **16 KB** LDROM (User Loader ROM)
  - **8 KB** Data Flash with power balance access and data scrambling technology. Clear data when tamper occurs automatically
  - **256 KB** SRAM, first 32 KB with hardware parity check (SRAM1: 32 KB, SRAM2: 128 KB, SRAM3: 96 KB)
  - **3 KB** OTP for general-purpose use (3 KB data + 1 KB lock bit)
  - **12 KB** secret OTP (for root keys, FVC, PLM and DPM)
  - **2 KB** non-volatile key storage (Flash) only accessed by key store
  - **16 KB** Secure Boot ROM embedded with enhanced secure boot loader based on root of trust mechanism
  - Up to 4 regions XOM blocks
  - ISP/ICP/IAP programming
  - External Bus Interface(EBI) supports maximum external address space of 1M Bytes, up to 3 chip selects and 8/16-bit external data bus
- **Clocks**
  - 4 to 24 MHz crystal oscillator (HXT)
  - 32.768 kHz crystal oscillator for RTC (LXT)
  - One Internal 12 MHz RC HIRC oscillator (variation < ±2% at -40℃~105℃) (HIRC12M)
  - One internal 48 MHz RC (HIRC48M)
  - One internal 1 MHz RC (MIRC 1M)
  - Internal 32.768 kHz RC with calibration (LIRC32K)
  - Supports one PLL up to 200 MHz for high performance system operation, sourced from HIRC and HXT
  - Internal 32.768 kHz LIRC in V_{BAT} domain for LXT clock accuracy and clock missing detection (LIRC1_32K)
  - Internal 4 MHz MIRC
- **Power management**
  - Supports power gating and ULPBench Mark targeting score is 180 for CP; 40 for PP
  - Normal run: 90 µA/MHz (LDO); 40 µA/MHz (DC-DC)
  - Power-down: 20 µA
  - Standby power-down: 2 µA
  - Deep Power-down: less than 0.1 µA (without V_{BAT})
  - V_{BAT} supply for RTC: 0.5 µA (80 bytes spare registers)
- **Timers and control**
  - Four 24-bit timers (Timer0~3), with up to 8 PWM channels
  - Twelve 16-bit timers (PWM0~1) with up to 12 enhanced PWM channels
  - Two 16-bit timers (BPWM0~1), with up to 12 PWM channels
  - Three 24-bit timers for ISO-7816-3
  - Two 24-bit SysTick timers: trusted system timer and Non-trusted system timer
  - Secure RTC supporting Calendar and Alarm function with secure spare registers protection capability
  - Two watchdog timers (one is Trusted region)
  - One window watchdog timer (Trusted region)
  - Low-power timer (System power down for PWM output)
  - Up to 2 quadrature encoder interfaces (QEI)
  - Up to 2 input capture timers (ECAP)
- **PDMA controller**
  - Two 8-ch PDMA controllers; PDMA0 is trusted PDMA and PDMA1 can be configured as trusted or Non-trusted PDMA
- **Security and integrity**
  - CRC calculation unit
  - 128-bit Unique ID (UID)
  - 128-bit Unique Customer ID (UCID)
  - True random number generator (TRNG)
  - Supports AES-256/SHA-512/HMAC-512/RSA-4096 and ECC accelerator with countermeasure for side-channel attack; AES supports CCM and GCM modes and GMAC
  - Supports China SM2/SM3/SM4 crypto algorithms
  - Supports NuSMP 2.0, including monotonic firmware version counter (FVM), Product Lifecycle

Management (PLM), Boot flag and Debug Port Management (DPM)
- Key store module embedded with 4 KB SRAM with power balance access and active shield protection technology.
- Tamper detection features for input voltage, external clock source and up to 6 tamper I/O pins
- Clear keys and data stored in spare register automatically when a tampering detected
- Internal 32.768 kHz LIRC dedicated for tamper engine (TLIRC)
- Privilege signal from SCU for master and slave peripherals privilege mode control
- 80 bytes spare registers in V_{BAT} domain

- **Analog**
  - One 12-bit, 6 MSPS @96 MHz SAR ADC (up to 16 channels)
  - Two 12-bit, 1MSPS DACs
  - Two rail-to-rail comparators (CMP)
  - Built-in temperature sensor
- **Communication interfaces**
  - Up to 6 UART interfaces (up to 12 MHz) with RS-485, IrDA, auto-flow control and LIN mode
  - Up to 2 USCI interfaces with UART, I^2C and SPI mode
  - Up to 3 I^2C interfaces (up to 1 Mbps) with SMBus/ PMBus
  - Up to 4 SPI-I^2S interfaces (up to 96 MHz) with SPI and I^2S mode
  - One Quad-SPI interface (up to 96 MHz)
  - One I^2S supports TDM multi-channel transmission
  - Up to 3 ISO 7816-3 smart card interfaces with smart card and UART mode
- **LCD Controller**
  - Supports 8x40 COM/SEG LCD display panel
  - Internal 1 MHz MIRC dedicated for LCD charge pump
- **Advanced connectivity**
  - USB 2.0 full speed OTG/Host/Device controller with on-chip PHY and embedded dual-buffer.
  - One CAN interface up to 1 Mbps (CAN 2.0A and 2.0B standard)
  - One Secure Digital I/O (SDIO)(up to 96 MHz clock rate)
- **Motor Interfaces**
  - Up to **2** quadrature encoder interfaces (QEI)
  - 2 input capture timers (ECAP)
- **Voltage Adjustable Interface**
  - Up to 6 I/O pins support VAI with supply V_{DDIO} from 1.7 to 3.6 V
- **Up to 80 I/O with interrupt capability**
  - 5V input tolerant I/O except for analog pins
- **128-bit Unique ID (UID)**
- **128-bit Customer ID (UCID)Packages (RoHS)**
  - LQFP 128-pin / 64-pin / 48-pin

3 BLOCK DIAGRAM

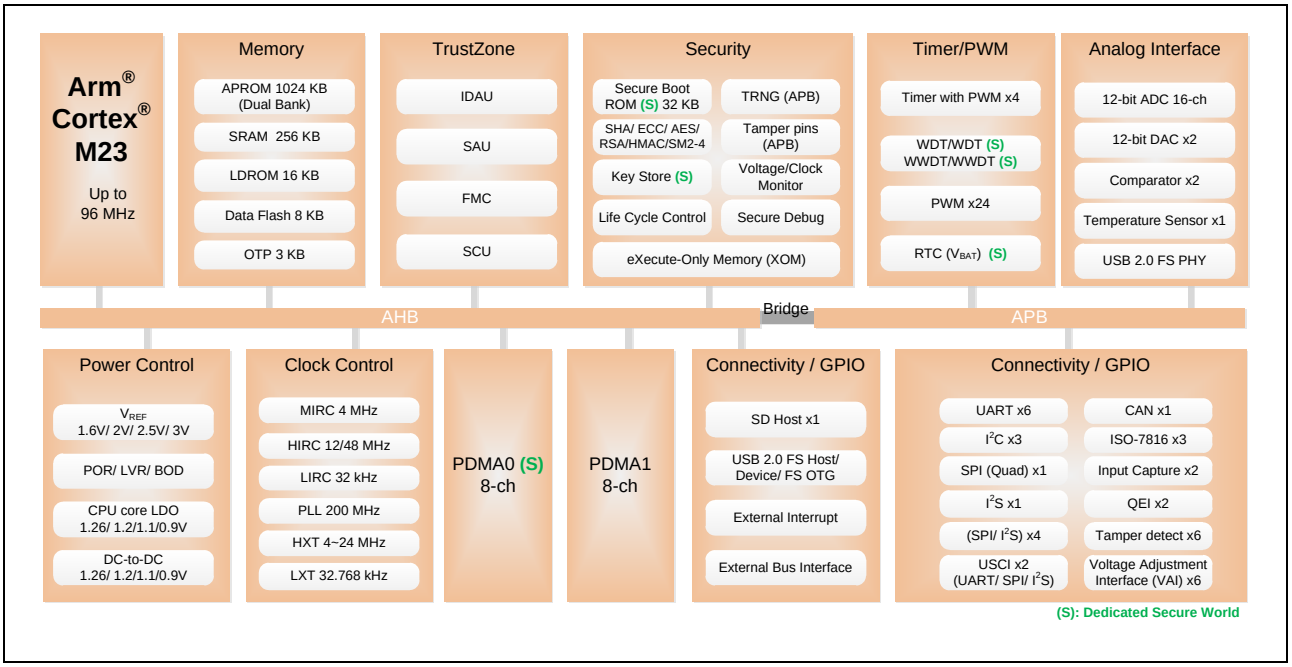

Figure 3-1 M2354 Block Diagram

4 PARTS INFORMATION

4.1 M2354 Series Selection Code

M23	54	K	J	F	A	E
Secure Core	**Line**	**Package**	**Flash**	**SRAM**	**Rev.**	**Temperature**
Cortex®-M23	**54:** Ultra Line **(Segment LCD)**	**L:** LQFP48 (7x7 mm) **S:** LQFP64 (7x7 mm) **K:** LQFP128 (14x14 mm)	**J:** 1024 KB	**F**: 256 kB		**E:** -40°C~105°C

Table 4-1 M2354 Series Selection Code

4.2 M2354 Series Selection Guide

PART NUMBER			M2354					
			LJFAE		SJFAE		KJFAE	
Flash (KB)			1024		1024		1024	
SRAM (KB)			256		256		256	
ISP Loader ROM (KB)			16					
I/O			40		50		106	
32-bit Timer			4					
Tamper I/O			1		1		6	
RTC			√					
Connectivity	LPUART		6					
	ISO-7816		3					
	Quad SPI	SPI/I²S	1	3	1	4	1	4
	I²S		1					
	I²C		3					
	USCI (UART/I²C/ SPI)		2					
	CAN		1					
	LIN		2					
	SDHC		1		1		1	
Crypto	TRNG		√					
	AES		√					
	ECC		√					
	SHA/HMAC		√					
	RSA		√					
Enhanced Security	FVC		√					
	DPM		√					
	PLM		√					
	Key Store		√					
Power Glitch Detector			√					
LCD (COMXSEG)			-		8 X 13		8 X 40	
16-bit Enhanced PWM			12					
16-bit Basic PWM			12					
QEI			2		2		2	
ECAP			1		1		1	
USB 2.0 FS OTG			√					
12-bit ADC			11		16		16	
12-bit DAC			2					
Analog Comparator			2		2		2	
External Bus Interface			√		√		√	
Package			LQFP48		LQFP 64		LQFP 128	

Table 4-2 NuMicro® M2354 Series Selection Guide

5 UTILITIES

5.1 Programmer and Debugger

Nu-Link	Basic full speed USB2.0 hardware debugger/programmer
Nu-Link-Pro	Advance hardware debugger/programmer with programming counter
Nu-Link 2.0	Advance high speed USB2.0 hardware debugger/programmer with multi-functions
Nu-Link-Gang	Off-line hardware programmer supports up to four chips programming for mass-production
ISP	In system programming, a software programming tool support UART/USB
ICP	In Chip Programming, a software programming tool support Nu-Link programmer

5.2 Development Environment

Programming IDE	Keil MDK, IAR, NuEclipse(GCC)
Software Package	Board Support Package(BSP), Sample Code,
Development IDE	NuTool PinView, NuTool PinConfig, NuTool ClockConfig, NuConsole
RTOS	Mbed, FreeRTOS, Amazon FreeRTOS, Ali-OS
HMI	Support emWin with font create tool and easy GUI builder

5.3 Development Board

EVB NuMaker	**Part Number**	**Feature**
NK-BEDM2354	M2354KJFAE	Support USB interface, CAN bus interface, COM/SEG LCD interface, Wi-Fi connectivity, SD card interface, Expand Connector, and Arduino Uno Interface

6 PROTECTION OVERVIEW FOR MCU APPLICATION SYSTEM

To ensure security quality of M2354 to be compliant with Arm® PSA TBSA-M specification, Nuvoton has developed a range of hardware and software technologies. These include hardware Ips and a lot of software tools/utilities. The most security features coverage is NuMicro® Secure Microcontroller Platform (NuSMP) including a range of hardware and software mixture technologies for security requirements for general purpose and IoT MCU security.

The following is a comparison table for M235x series with detailed chip security features.

Category	Item	M2351	M2354
Secure Boot ROM	Secure Bootloader(based on ECDSA signature)	✓	✓
	Secure firmware update (OTA)	✓	✓
	Driver APIs	✓	✓
	Debug Authentication (temporarily unlock)	✓	✓
Security Reference Code / Lib / Tool	TrustZone reference code (NuBL2, NuBL32)	✓	✓
	Key Generation Tool	✓	✓
	Image Singing Tool	✓	✓
	Key Provision Tool	✓	✓
Isolation	Peripheral privileged mode	✓	✓
	TrustZone partition for Cortex-M	✓	✓
Flash Memory Protection	Flash Lock (general read protection)	✓	✓
	eXecute Only Memory	✓	✓
	Dual bank (with bank remap)	✓	✓
	Flash Protection Region (write protection)	✓	✓
Crypto Processors	DES/3DES	✓	
	AES-256	✓	✓
	AES CCM, GCM and GMAC		✓
	ECC (Key generation, ECDH-ECDSA)	✓	✓
	RSA-4096		✓
	Side Channel Attacks mitigation of AES, RSA, ECC		✓
	SHA1/SHA2-384	✓	✓
	SHA2-512, HMAC-512		✓
	SM2/3/4*		✓
	TRNG	✓	✓

	Cryptographic key store with chip level Active Shield		✓
Device Identity	Unique ID	✓	✓
	Unique Customer ID	✓	✓
Anti-Tamper	Tamper Pin Detection	✓	✓
	RTC backup registers	✓	✓
Environment Sensor	Temperature sensors		✓
	Enhanced clock monitor		✓
	Voltage glitch detection		✓
Platform Security (Arm PSA TBSA-M)	Booting Status Monitor	✓	✓
	Life Cycle Management	✓	✓
	Firmware Version Counter (FVC)	✓	✓
	Debug Port Management (DPM)	✓	✓
*Chinese national cryptography standard			

Table 6-1 M235x Series MCU Security Detail Features

7 REVISION HISTORY

Date	Revision	Description
2020.07.15	1.00	Initial version.
2020.12.25	1.01	With new product brief template adoption

Important Notice

Nuvoton Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, "Insecure Usage".

Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, the control or operation of dynamic, brake or safety systems designed for vehicular use, traffic signal instruments, all types of safety devices, and other applications intended to support or sustain life.

All Insecure Usage shall be made at customer's risk, and in the event that third parties lay claims to Nuvoton as a result of customer's Insecure Usage, the customer shall indemnify the damages and liabilities thus incurred by Nuvoton.