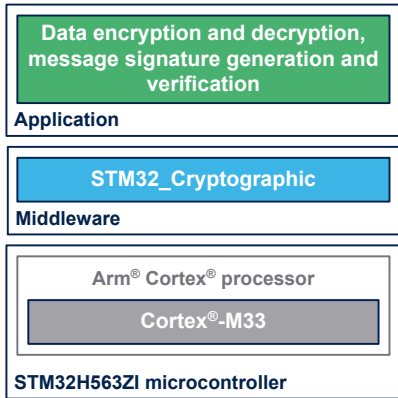


# STM32 post-quantum cryptographic library software expansion for STM32Cube



Product status
X-CUBE-PQC



## Features

### X-CUBE-CRYPTOLIB security algorithms

- Cipher encryption and decryption
- Digest generation
- Message authentication code (MAC) generation
- Elliptic curves based on key generation, signature, and verification
- Elliptic curves Diffie-Hellman
- RSA signature, verification, encryption, and decryption
- Deterministic random bit generator (DRGB)

### PQC public key cryptography

- Stateful hash-based signatures (HBS):
  - LMS digital signature verification

## Description

With the advent of quantum computers, traditional asymmetric cryptographic algorithms such as RSA, ECC, DH, ECDH, and ECDHE become vulnerable. In response, NIST has selected a new set of algorithms designed to be resistant to quantum computing attacks.

The STM32 post-quantum cryptographic library package (X-CUBE-PQC) includes all the major security algorithms for encryption, hashing, message authentication, and digital signing. This enables developers to satisfy application requirements for any combination of data integrity, confidentiality, identification/authentication, and nonrepudiation. The library includes the PQC Leighton-Micali signature (LMS) verification method, which is used mainly for secure boot code authentication.

The library includes firmware functions for the STM32H563ZI microcontroller, based on the Arm® Cortex®-M33 processor, and all cryptographic functions of STMicroelectronics X-CUBE-CRYPTOLIB. For more details, refer to the STM32 cryptographic library dedicated pages of the STM32 MCU wiki at [wiki.st.com/stm32mcu](http://wiki.st.com/stm32mcu).

Most of the widely used algorithms, except LMS, are certified according to the NIST cryptographic algorithm validation program (CAVP), helping customers to prove quickly and cost-effectively the security of their new products.

Full details are available online at the NIST CSRC algorithm validation lists website, selecting the CAVP web page.

This package contains an example of LMS signature verification using the STM32 cryptographic accelerator. To benefit from all other cryptographic examples, refer to the X-CUBE-CRYPTOLIB Expansion Package.

# 1 General information

The X-CUBE-PQC Expansion Package runs on the STM32H563ZI microcontroller, based on the Arm® Cortex®-M33 processor with Arm® TrustZone®.

*Note: Arm and TrustZone are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All other trademarks are the property of their respective owners.*



## 1.1 Ordering information

X-CUBE-PQC is available for free download from the [www.st.com](http://www.st.com) website.

## 1.2 NIST algorithm validation lists

Refer to [Table 1](#) for access to the certification listing on the National Institute of Standards and Technology (NIST) portal.

**Table 1. NIST CSRC algorithm validation lists**

Cortex® architecture	Optimization type	CAVP link
Cortex®-M33	Size	<a href="https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13548">csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13548</a>
Cortex®-M33	Speed	<a href="https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13493">csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13493</a>

## 1.3 What is STM32Cube?

**STM32Cube** is an STMicroelectronics original initiative to improve designer productivity significantly by reducing development effort, time, and cost. STM32Cube covers the whole STM32 portfolio.

STM32Cube includes:

- A set of user-friendly software development tools to cover project development from conception to realization, among which are:
  - **STM32CubeMX**, a graphical software configuration tool that allows the automatic generation of C initialization code using graphical wizards
  - **STM32CubeIDE**, an all-in-one development tool with peripheral configuration, code generation, code compilation, and debug features
  - **STM32CubeCLT**, an all-in-one command-line development toolset with code compilation, board programming, and debug features
  - **STM32CubeProgrammer (STM32CubeProg)**, a programming tool available in graphical and command-line versions
  - **STM32CubeMonitor (STM32CubeMonitor, STM32CubeMonPwr, STM32CubeMonRF, STM32CubeMonUCPD)**, powerful monitoring tools to fine-tune the behavior and performance of STM32 applications in real time
- **STM32Cube MCU and MPU Packages**, comprehensive embedded-software platforms specific to each microcontroller and microprocessor series (such as STM32CubeH5 for the STM32H5 series), which include:
  - STM32Cube hardware abstraction layer (HAL), ensuring maximized portability across the STM32 portfolio
  - STM32Cube low-layer APIs, ensuring the best performance and footprints with a high degree of user control over hardware
  - A consistent set of middleware components such as ThreadX, FileX, LevelX, NetX Duo, USBX, USB PD, mbed-crypto, MCUboot, and OpenBL
  - All embedded software utilities with full sets of peripheral and applicative examples
- **STM32Cube Expansion Packages**, which contain embedded software components that complement the functionalities of the STM32Cube MCU and MPU Packages with:
  - Middleware extensions and applicative layers
  - Examples running on some specific STMicroelectronics development boards



---

## 2 License

---

X-CUBE-PQC is delivered under the [SLA0048](#) software license agreement and its Additional License Terms.

## Revision history

**Table 2. Document revision history**

Date	Revision	Changes
05-Mar-2025	1	Initial release.

**IMPORTANT NOTICE – READ CAREFULLY**

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to [www.st.com/trademarks](http://www.st.com/trademarks). All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2025 STMicroelectronics – All rights reserved