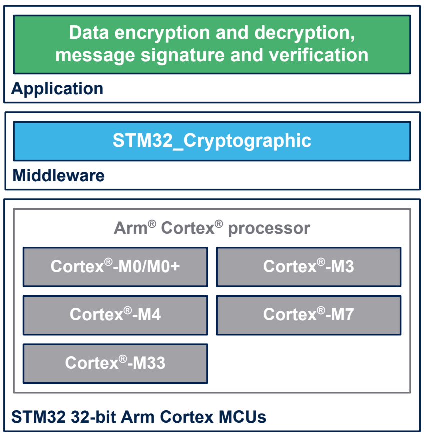
X-CUBE-CRYPTOLIB

Data brief

STM32 cryptographic library software expansion for STM32Cube



Product status link
X-CUBE-CRYPTOLIB

Features

- Cipher encryption and decryption:
  - AES: CBC, CCM, CFB, CTR, ECB, GCM, OFB, XTS, KeyWrap
  - SM4: CBC, CFB, CTR, ECB, OFB
  - Chacha-Poly1305
- Digest generation:
  - SHA-1
  - SHA-2: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256
  - SHA-3: SHA3-224, SHA3-256, SHA3-384, SHA3-512
  - SM3
  - SHAKE
- Message authentication code (MAC) generation:
  - HMAC:
    - SHA-1
    - SHA-2: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256
    - SM3
  - AES: CMAC
  - KMAC: SHAKE
- Elliptic curves based on key generation, signature and verification:
  - Elliptic curve digital signature algorithm (ECDSA): NIST-R (P-224, P-256, P-384, P-521), NIST-K P-256, BRAINPOOL R/T (P-160, P-192, P-224, P-256, P-320, P-384, P-512), ANSSI P-256
  - Edwards-curve digital signature algorithm (EdDSA): Ed448, Ed25519
  - SM2 digital signature algorithm: OSCCA 256-bits curve
- Elliptic curves Diffie-Hellman:
  - Curve448, curve25519
  - NIST-R (P-224, P-256, P-384, P-521), NIST-K P-256, BRAINPOOL R/T (P-160, P-192, P-224, P-256, P-320, P-384, P-512), ANSSI P-256
- RSA signature, verification, encryption and decryption:
  - PKCS#1 v1.5 and v2.2
  - Chinese remainder theorem (CRT) key representation
  - Hash method:
    - SHA-1
    - SHA-2: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256
- Deterministic random bit generator (DRBG):
  - CTR-DRBG

1 Description

The STM32 cryptographic library package (X-CUBE-CRYPTOLIB) includes all the major security algorithms for encryption, hashing, message authentication, and digital signing, enabling developers to satisfy application requirements for any combination of data integrity, confidentiality, identification/authentication, and non-repudiation.

The library includes firmware functions for the STM32 microcontrollers in the STM32F0 Series, STM32F1 Series, STM32F2 Series, STM32F3 Series, STM32F4 Series, STM32F7 Series, STM32G0 Series, STM32G4 Series, STM32H7 Series, STM32L0 Series, STM32L1 Series, STM32L4 Series, STM32L4+ Series, STM32L5 Series, STM32U5 Series, STM32WB Series and STM32WL Series depending on their Arm® Cortex®-M processor. For more details, refer to the *STM32 cryptographic library* dedicated pages of the STM32 MCU wiki at wiki.st.com/stm32mcu.

Most of the well-used algorithms are certified according to the US 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.

In this package there are examples for each algorithm for popular development tools including IAR Systems® EWARM (IAR Embedded Workbench®), Keil® MDK-ARM, and GCC -based IDEs such as STMicroelectronics STM32CubeIDE.

To benefit from STM32 cryptographic accelerators, refer to STM32Cube MCU and MPU package hardware abstraction layer (HAL) functions and examples.

2 General information

The X-CUBE-CRYPTOLIB runs on STM32 microcontrollers based on Arm® Cortex® cores.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

2.1 Ordering information

X-CUBE-CRYPTOLIB is available for free download from the *www.st.com* website.

2.2 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®-M0/M0+	Size	csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13549
Cortex®-M0/M0+	Speed	csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13550
Cortex®-M3	Size	csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13546
Cortex®-M3	Speed	csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13547
Cortex®-M4	Size	csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13544
Cortex®-M4	Speed	csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13545
Cortex®-M7	Size	csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13542
Cortex®-M7	Speed	csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13543
Cortex®-M33	Size	csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13548
Cortex®-M33	Speed	csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13493

2.3 What is STM32Cube?

STM32Cube is an STMicroelectronics original initiative to significantly improve designer's productivity 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
  - 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 STM32CubeL4 for the STM32L4 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 FAT file system, RTOS, USB Host and Device, TCP/IP, Touch library, and Graphics
  - 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

3 License

X-CUBE-CRYPTOLIB is delivered under the SLA0048 software license agreement and its Additional License Terms.

Revision history

Table 2. **Document revision history**

Date	Revision	Changes
1-Sep-2015	1	Initial release.
9-Dec-2015	2	Updated *Features* and *Description* to introduce a new cryptographic firmware version.
15-Dec-2015	3	Updated *Description* and *Section 2: Ordering information*.
7-Jul-2016	4	Updated *Features* and *Description* to introduce the list of certified algorithms.
20-Nov-2020	5	Extended the document scope to the STM32WL Series. Added the *Product information* and *License* sections and the cover picture. Updated *Description*.
12-Jan-2021	6	Updated the document title. Updated in *Product information* the versions for the STM32F0 Series, STM32G0 Series, STM32L0 Series, STM32L5 Series and STM32WL Series.
14-May-2021	7	Extended the number of security algorithms in STM32 cryptographic library with full NIST validation according to the Arm® Cortex®-M processor: • Updated the cover picture • Updated *Features* and *Description* • Added *NIST algorithm validation lists* Updated *License*. Removed *Product information*.
21-Jul-2021	8	Extended the document scope to the STM32U5 Series: updated Description. Updated License with the Additional License Terms.

IMPORTANT NOTICE – PLEASE 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 acknowledgement.

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, please refer to 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.