STM32 cryptographic library software expansion for STM32Cube

**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
The STM32 cryptographic library package \textit{(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, STM32WB Series and STM32WL Series depending on their Arm\textsuperscript{®} Cortex\textsuperscript{®}-M processor. For more details, refer to the \textit{STM32 cryptographic library} dedicated pages of the STM32 MCU wiki at wiki.st.com/stm32mcu.

This firmware is classified ECCN 5D002.c.1.

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.

\textbf{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\textsuperscript{®} EWARM (IAR Embedded Workbench\textsuperscript{®}), Keil\textsuperscript{®} 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>
<thead>
<tr>
<th>Cortex® architecture</th>
<th>Optimization type</th>
<th>CAVP link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cortex®-M0/M0+</td>
<td>Size</td>
<td>csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13549</td>
</tr>
<tr>
<td>Cortex®-M0/M0+</td>
<td>Speed</td>
<td>csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13550</td>
</tr>
<tr>
<td>Cortex®-M4</td>
<td>Speed</td>
<td>csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13545</td>
</tr>
<tr>
<td>Cortex®-M33</td>
<td>Speed</td>
<td>csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13493</td>
</tr>
</tbody>
</table>
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
X-CUBE-CRYPTOLIB is delivered under the Mix Ultimate Liberty+OSS+3rd-party V1 software license agreement (SLA0048).

The software components provided in this package come with different license schemes as shown in Table 2.

### Table 2. Software component license agreements

<table>
<thead>
<tr>
<th>Software component</th>
<th>Copyright</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>STM32_Cryptographic middleware</td>
<td>STMicroelectronics</td>
<td>Proprietary</td>
</tr>
<tr>
<td>Board support package (BSP)</td>
<td>STMicroelectronics</td>
<td>BSD-3-Clause</td>
</tr>
<tr>
<td>Cortex®-M CMSIS</td>
<td>Arm Limited</td>
<td>Apache License 2.0</td>
</tr>
<tr>
<td>HAL/LL STM32G0, STM32G4, STM32H7, STM32L0, STM32L1, STM32L4, STM32L4+, STM32L5, STM32WB and STM32WL</td>
<td>STMicroelectronics</td>
<td>BSD-3-Clause</td>
</tr>
<tr>
<td>Project examples</td>
<td>STMicroelectronics</td>
<td>Proprietary</td>
</tr>
</tbody>
</table>
### Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-Sep-2015</td>
<td>1</td>
<td>Initial release.</td>
</tr>
<tr>
<td>9-Dec-2015</td>
<td>2</td>
<td>Updated Features and Description to introduce a new cryptographic firmware version.</td>
</tr>
<tr>
<td>15-Dec-2015</td>
<td>3</td>
<td>Updated Description and Section 2: Ordering Information.</td>
</tr>
<tr>
<td>7-Jul-2016</td>
<td>4</td>
<td>Updated Features and Description to introduce the list of certified algorithms.</td>
</tr>
<tr>
<td>20-Nov-2020</td>
<td>5</td>
<td>Extended the document scope to the STM32WL Series. Added the Product information and License sections and the cover picture. Updated Description.</td>
</tr>
<tr>
<td>12-Jan-2021</td>
<td>6</td>
<td>Updated the document title. Updated in Product information the versions for the STM32F0 Series, STM32G0 Series, STM32L0 Series, STM32L5 Series and STM32WL Series.</td>
</tr>
</tbody>
</table>
| 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. |