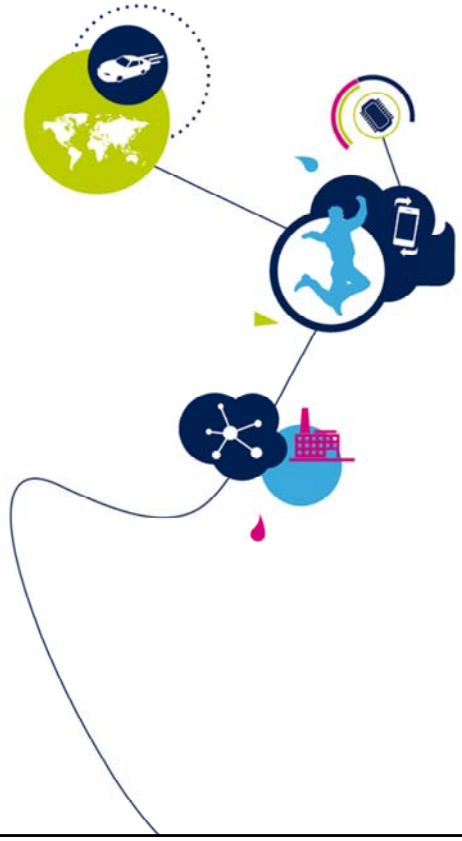
STM32L5 - OTFDEC

On-The-Fly Decryption Engine
Revision 1.0

Changes in blue or with * changes *

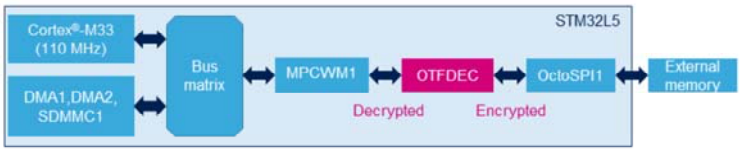
life.augmented



Hello, and welcome to this presentation of the OTFDEC, which is included in STM32L562 microcontrollers.

Overview

- On-the-fly decryption during OctoSPI memory-mapped read operations (single or multiple)
  - Use of AES in counter (CTR) mode to achieve lowest possible latency
- OTFDSEC location:



Application benefits

- External flash protection
- Up to four independent encrypted regions
- Region configuration write locking mechanism

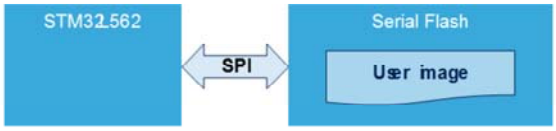
life.augmented

Original purpose of OTFDEC is to protect the confidentiality of read-only firmware libraries stored in external SPI NOR Flash devices.
The OTFDEC performs on-the-fly decryption during OCTOSPI memory-mapped read operation. Any read access size down to the byte is supported.
The OTFDEC is located between the Memory Peripheral Controller Watermark (MPCWM1), which is a part of the GTZC in charge of defining non-secure areas in the external memory and the OctoSPI1 that controls the access to an external serial flash.
Advanced Encryption Standard (AES) -128-bit algorithm in counter mode is implemented, to achieve the lowest possible latency.
As a consequence, each time the content of one encrypted region is changed the entire region must be re-encrypted with a different cryptographic context (key or initialization vector).

Up to four independent regions can be defined, each with their own 128-bit key and initialization vector information (64-bit application nonce and 16-bit encrypted library version). A write locking mechanism prevents any further reconfiguration of region parameters.

External Flash protection

- User wants to protect code and data stored in external Flash
  - External Flash can be unsoldered and then soldered again on new boards
  - External Flash standard SPI bus can be spied using probes



- User wants protection with a minimum impact on performances
  - AES algorithm consumes a lot of cycle to process blocks of data

life.augmented

The purpose of the OTFDEC peripheral is to protect the user code and data that are stored in the external serial flash memory.
If the image is stored unencrypted, it is easy to read it by either de-soldering the flash device then re-soldering it on another board or by spying the traffic on the SPI bus by using a logic analyzer or an oscilloscope.
Consequently the image stored in the flash memory should be encrypted then decrypted on the fly during run-time reads.
The latency caused by the decryption should be minimized.
The OTFDEC has been designed to tackle these objectives.

External Flash protection with OTFDEC

4

- The OTFDEC is a new peripheral within STM32L5 that is able to decrypt with low latency code or data stored within external SPI Flash
  - OTFDEC also supports a global encryption mode
- Code + data are protected within external flash up to OTFDEC output to STM32L5 masters
- The OTFDEC stands before OctoSPI from STM32 master perspective and intercepts therefore all data read & write and instruction fetch transactions targeting external Flash
- After OTFDEC setup, read/fetch transactions to external flash via OTFDEC are transparent from STM32 masters point of view (no decryption needed)

life.augmented

The OTFDEC is a new IP implemented in the STM32L562, able to decrypt with low latency code and data stored within an external flash. It also supports an encryption mode.
The encryption process must follow the sequence described in the reference manual. When encryption mode is selected flash on-the-fly decryption for all regions is de-activated.
Since the decryption is done internally by the microcontroller, the data transferred over the OctoSPI bus is encrypted. This is a countermeasure against flash unsoldering and bus spying.
The OTFDEC is a companion IP of the OctoSPI peripheral. It intercepts any data read/write and instruction fetch that targets the external flash.
Decryption is transparent to the Cortex-M33 core. Data and instructions that the processor receives have been decrypted in hardware by the OTFDEC.

OTFDEC features (1/2)

5

- Protect confidentiality of external :
  - Read-only code, read-only data + code areas, that are decrypted on the-fly
  - Four independent and non-overlapping encrypted regions can be defined
- AES 128-bit cipher in counter mode is used to achieve the lowest possible latency
  - Access minimum granularity: 8-bit
- Each region is defined by:
  - A secret key and its public 8-bit CRC
  - Public diversification data: 64-bit application info + 16-bit library version
- Shared AHB interface (data ciphering & register programming)

life.augmented

The OTFDEC protects confidentiality of external read only code and read only data + code areas.
They are decrypted on the fly.
Four independent and non-overlapping encrypted regions can be defined.
The AES 128-bit cipher in counter mode is used to achieve the lowest possible latency.
Access minimum granularity is 8 bits.
Each regions is defined by a 128-bit secret key, and its public 8-bit CRC.
Initialization vector of each region is built by OTFDEC using a 64-bit application information and a 16-bit library version.
The user can define this information as the public diversification data.
The OTFDEC has a unique AHB slave interface, used to access control and status registers and also to transfer data to encrypt and decrypt data.

OTFDEC features (2/2)

6

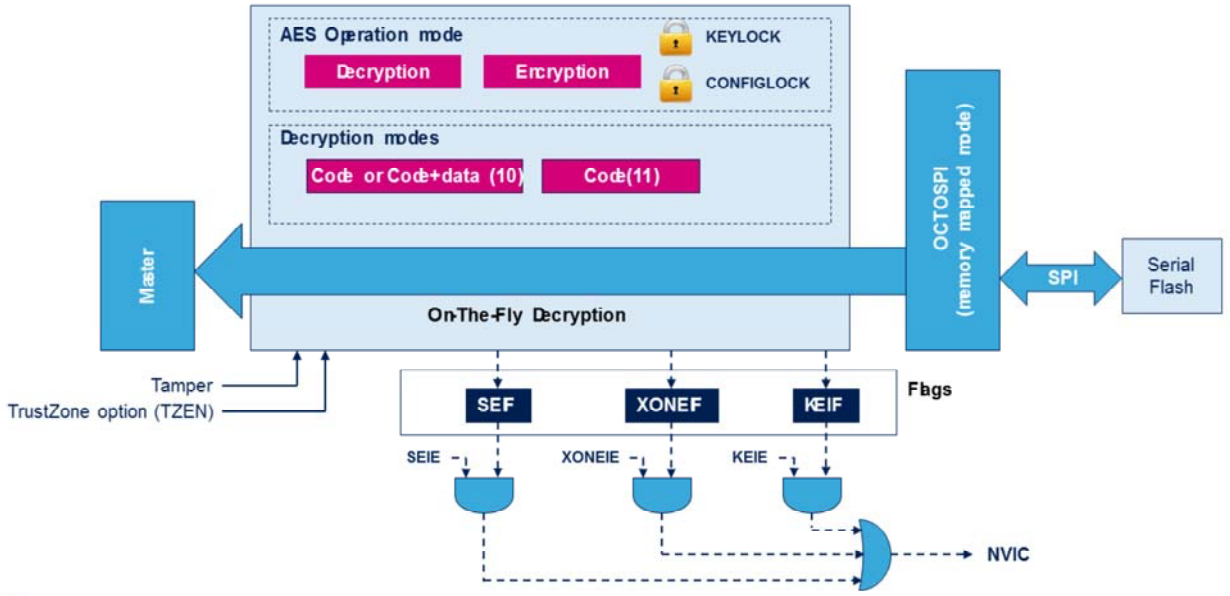
- OTFDEC operating modes per region:
  - MODE=10: code or data accesses
    - Standard AES encryption, can be embedded in tools or application firmware
  - MODE=11: instruction fetch only with enhanced encryption
    - Standard AES with additional layer of protection (proprietary). On-chip encryption must be used.
- Per-region security mechanisms
  - Write-only key registers, write protection until next reset (KEYLOCK & CONFIGLOCK)
- Global security mechanisms
  - Key erase in case of intrusion, RDP regression or MODE change
  - TrustZone-aware peripheral (register writes always secure when TZEN=1)
  - Privileged-only accesses when PRIV bit is set in OTFDEC_PRIVCFGR

life.augmented

For each region, the operating mode has to be selected.
If the region contains both code and data, the MODE field of the region configuration register has to be set to binary value 10. Standard AES encryption algorithm is used, hence encryption process can be embedded in code generation tools or application firmware for run-time encryption.
If the region only contains instruction, the MODE field of the region configuration register could be set to binary value 11. In this case an additional layer of protection is added on top of the standard AES encryption algorithm, hence encryption process cannot be embedded in software tools (OTFDEC must be used to perform the encryption).
The configuration of each region can be independently locked to prevent any further modification. Both the 128-bit key and the configuration parameters can be locked.
All key registers are write only, and are automatically erased in case of intrusion detected by tampers, Readout Protection (RDP) regression or MODE field change.

OTFDEC is a TrustZone-aware peripheral: all writes to its registers must be secure when security is activated in the product (TZEN=1).
When PRIV bit is set in OTFDEC_PRIVCFGR only privileged accesses are granted when accessing most OTFDEC registers.

OTFDEC Block Diagram

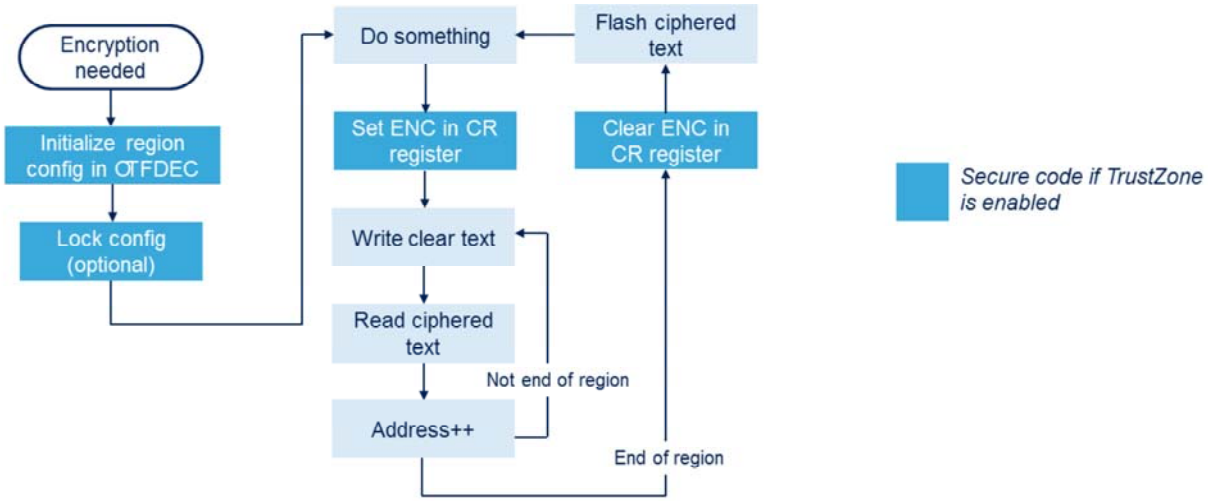


The principle of OTFDEC is to analyze all AHB read transfers on the associated AHB bus.
If the read request is within one of the four regions programmed in OTFDEC the control logic triggers a keystream computation based on AES algorithm in counter mode.
This keystream is then used to decrypt on-the-fly the data present in the read transfer from the OCTOSPI AHB master, tying low the HREADYOUT signal of this master while the keystream information is being computed (this takes up to 11 cycles).
Any access outside the enabled OTFDEC regions belongs to a non-encrypted region.
As OTFDEC is used in conjunction with OCTOSPI it is mandatory to access the flash memory using the memory map mode of the flash controller.
In the region configuration register, the MODE bits define the OTFDEC operating mode (standard or enhanced

encryption).
The OTFDEC can also be used for encrypting data using either the standard AES algorithm or the enhanced encryption algorithm.
A Tamper detection, a RDP regression or a MODE bits change automatically erases the keys.
The OTFDEC can assert an interrupt to the NVIC for three possible causes: Security error, Key error and Execute-only or execute while encryption error. Each of these causes has a dedicated flag and interrupt enable bit.

OTFDEC encryption

- User firmware is responsible for managing OTFDEC encryption mode and performing external Flash Programming

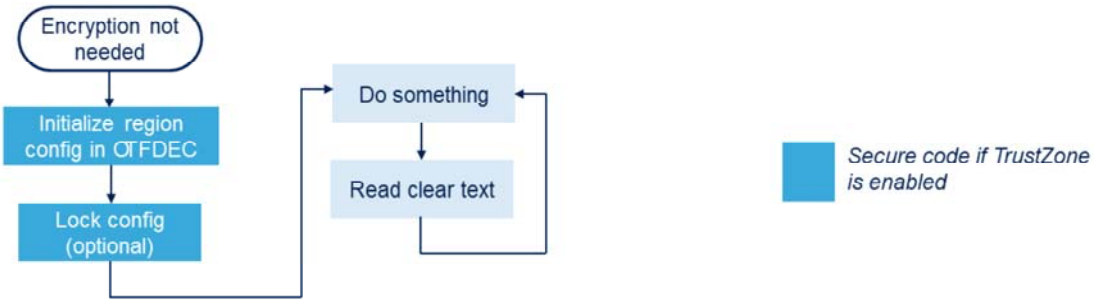


The ciphered data is stored in RAM.
This slide describes the sequence used to encrypt the contents of a memory buffer.
It has to be implemented in secure code when TrustZone is enabled.
User firmware is responsible for external Flash Programming.

OTFDEC decryption

9

- At STM32L5 reset, during the boot sequence, the user firmware must:
  - Load keys within OTFDEC key registers for each OTFDEC region
  - Lock OTFDEC configuration (e.g. keys)
- Then on-the-fly decryption is ready



The user firmware is in charge of the following initializations during the boot sequence:

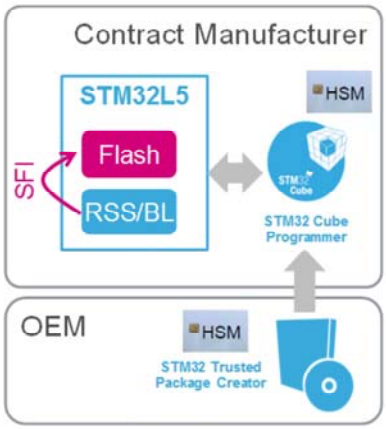
- Loading keys within OTFDEC key registers for each OTFDEC region
- Loading nonce, version, address start and address end information for each OTFDEC region
- Set REG_EN bits
- Locking OTFDEC configuration above (recommended)

Then on-the-fly decryption is ready.

User firmware must be secure if security is activated on the product (TZEN=1).

Secure firmware install with OTFDEC (1)

- Secure firmware install (SFI) is a global solution for STM32L5 Series of microcontrollers, allowing secure and counted installation of OEM firmware in untrusted production environment (such as OEM contract manufacturer)
- When external Flash memory is targeted by SFI, OEM firmware is encrypted with an external firmware and data AES key
- OTFDEC can be used to encrypt the external firmware, for example with a device unique key
  - This option is mandatory when MODE=11 (enhanced) is selected for the region
  - It is illustrated on the next slide
- Refer to AN4992 for more details



Secure firmware install (SFI) is a global solution for STM32L5 Series of microcontrollers, allowing secure and counted installation of OEM firmware in untrusted production environment (such as OEM contract manufacturer). OEM firmware protected by SFI can be store in the device's embedded flash or encrypted in external flash connected via OCTOSPI.

When external Flash memory is targeted by SFI, OEM firmware code must be encrypted with an external firmware and data AES key. This key can be:

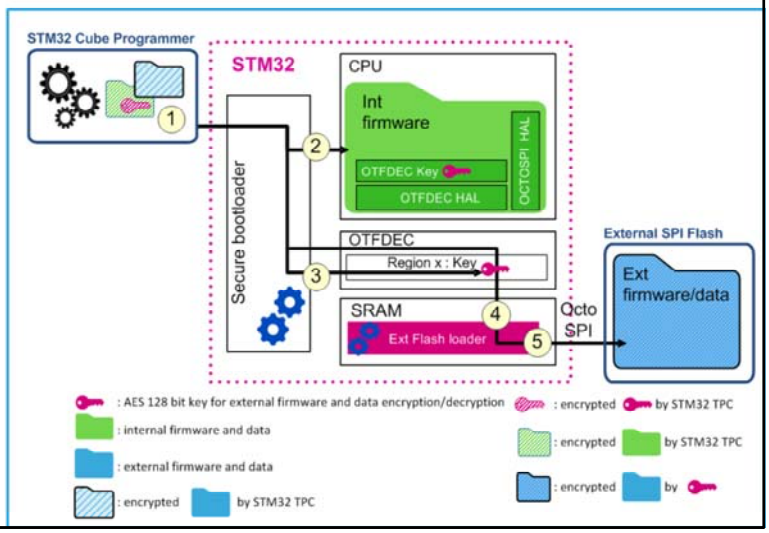
- Common to all devices (in this case tools could perform the encryption if OFTDEC MODE=10), or
- Unique per device (in this case firmware is encrypted inside the device, mandatory if OTFDEC MODE=11)

Encryption on-chip using OTFDEC is illustrated on the following slide.

For more information please refer to application note AN4992 for secure firmware install (SFI) solutions.

Secure firmware install with OTFDEC (2)

1. Create an SFI image with STM32 Trusted Package Creator (TPC)
   - Internal firmware and data (including external Flash memory drivers)
   - External firmware and data *AES key*
   - External firmware and data
2. Internal Flash memory programming
3. External firmware and data *AES key* programming in OTFDEC peripheral
   - Alternatively such key(s) can be managed locally to the device, not globally in the flashing tools.
4. External Flash memory chunk encryption
5. External Flash memory programming by the user's firmware



This slide represents the sequence where the STM32 secure bootloader handles both internal firmware installation and external firmware installation with a global external Flash memory AES key and the help of an external Flash memory loader. The numerical steps are represented on the schematic.

(1) Create an SFI image using STM32 Trusted Package Creator (TPC), with a) internal firmware and data (including external Flash memory drivers), b) external firmware and data AES key, and c) external firmware and data

(2) Internal Flash memory programming, as described in the STM32L5 RSS training.

(3) External firmware and data AES key programming in OTFDEC peripheral. Alternatively to what is drawn on the slide this key can be managed locally to the device, not globally in the flashing tools.

(4) External Flash memory chunk encryption

(5) External Flash memory programming by the user's

firmware

Afterward, during each secure boot, the secure internal firmware first copies the AES firmware and data key(s) in write-only OTFDEC key registers, then activates the OTFDEC region tied to those keys. At this point the CPU can seamlessly read/fetch data/code from external Flash memory once the OCTOSPI driver has been initialized.

Trustzone-aware peripherals: OTFDEC

- TrustZone support
  - When TrustZone security is activated (TZEN=1 in the FLASH_OPTR register) most registers are writable only by a secure application
- Privileged access support
  - Additional access control is available on top of TrustZone security. It is available whether or not TrustZone security is activated
    - When PRIV bit is set in PRIVCFG register access to the whole OTFDEC configuration becomes privileged-only
  - Default state: privileged and unprivileged access to OTFDEC are allowed

The OTFDEC is a TrustZone-aware peripheral. When TrustZone is disabled, only the privilege attribute is relevant. By setting the PRIV bit in the privilege configuration register (PRIVCFGR), unprivileged reads return zero and unprivileged writes are ignored.
When TrustZone is enabled, non-secure write access to OTFDEC registers are discarded.
Consequently when TrustZone is enabled, OTFDEC regions can only be programmed by secure applications.
The privilege attribute can also be set when TrustZone is enabled.

Interrupts

Interrupt event	Description
Security error	Illegal read to key registers Illegal write to key registers while KEYLOCK=1 Illegal write to a region's configuration while CONFIGLOCK=1
Execute-only Execute while encryption	Read access to a region with enhanced encryption selected (MODE[1:0]=11) Executing while encryption is enabled (ENC=1)
Key error	Read request to an encrypted region while its key registers are null or not properly initialized (KEYCRC=0x0). ➢ Source of the error can be an incorrect key loading sequence (see KEYCRC in OTFDEC_RxCFGR) or erased in case of intrusion detected by tampers, Readout Protection (RDP) regression or MODE field change Such read requests return 0x0, without bus error.

The OTFDEC has 3 interrupt sources.
The security error is raised when an attempt to read key registers is detected or when an attempt to write keys while the KEYLOCK bit is set or when an attempt to reconfigure a region while the CONFIGLOCK bit is set.
When enhanced encryption is selected (MODE=11) the execute-only error is raised when a read access to an execute only region is attempted.
When encryption mode is selected (ENC=1) the execute while encryption error is raised when code is fetched to any protected region.
The key error is raised when a read request is attempted to a region whose key registers are null or not properly programmed (KEYCRC=0x0). Key error can happen due to an incorrect key register writing sequence. It can also occur in case of intrusion detected by tampers, Readout

Protection (RDP) regression or MODE field change.

Low-power Modes

Mode	Description
Run	Active.
Sleep	Active. Peripheral interrupts cause the device to exit Sleep mode.
Low-power run	Active.
Low-power sleep	Active. Peripheral interrupts cause the device to exit Low-power sleep mode.
Stop 0	Frozen. Peripheral registers content is kept.
Stop 1	
Stop 2	
Standby	Powered-down. The peripheral must be reinitialized after exiting Standby mode.
Shutdown	Powered-down. The peripheral must be reinitialized after exiting Shutdown mode.

The OTFDEC is active in Run, Sleep, Low-power run and Low-power sleep mode. An OTFDEC interrupt can cause the device to exit Sleep or Low-power sleep mode.
In Stop0, Stop1 or Stop2 mode, the OTFDEC is frozen, and its registers content is maintained.
In Standby or Shutdown mode, the OTFDEC is powered-down and it must be reinitialized afterward.

Related peripherals

15

- Refer to these trainings linked to this peripheral for more information
  - Global TrustZone® Controller (GTZC)
  - OctoSPI interface (OCTOSPI)
  - Nested Vectored Interrupt (NVIC)
  - Memory protection (MEMPROTECT)
  - Root Security Services (RSS)
- For more details and additional information, refer to the following
  - AN4992: Overview of secure firmware install (SFI)

life.augmented

The OTFDEC module has relationships with the following other module:

- Global TrustZone Controller
- OctoSPI interface
- Nested Vectored Interrupt Controller
- Memory protection
- Root Security services (with SFI information)

For more details on SFI, please refer to application note AN4992 about Overview of secure firmware install (SFI).