Hello, and welcome to this presentation of the STM32F7 cryptographic processor.
This peripheral supports the Data Encryption Standard (DES), the Triple-DES and the Advanced Encryption Standard (AES) in several operating modes.
Authentication and confidentiality are required for most communication channels. Cryptography is then widely used but is very demanding in terms of processing for a CPU. STM32F7 microcontrollers embed a hardware accelerator for the efficient computation of block-based algorithms DES and AES. These well-known standards are suitable for symmetric cryptography involving a shared key between both parties.
The cryptographic processor supports the Data Encryption Standard (DES), the Triple-DES and the Advanced Encryption System (AES) in several operating modes described in the next slides. Both standards are part of the block-cipher algorithm family. DES uses a 56-bit key while AES, which is more robust, can be used with a key of 128, 192 or 256 bits. A full data flow can be automated with the help of the Direct memory access controller (DMA).
Data Encryption Standard works on a data block of 64 bits; input data is encrypted or decrypted using the same 56-bit key.

Large messages are divided in several blocks of 64 bits that are chained together following one of the two next modes of operation: Electronic codebook (ECB) or cipher block chaining (CBC).
ECB is a direct implementation block after block with no dependencies between them. It can be used safely with small messages.
For larger messages, CBC is preferred since it efficiently randomizes the encrypted output.

Triple DES, shown in the diagram, consists in chaining three consecutive DES operations for the same block of 64 bits with either the same key or with three different keys. As with DES, block chaining can follow either ECB or CBC.
Advanced Encryption Standard works on block of 128 bits. Encryption or decryption can be done using a key of 128, 192 or 256 bits. A full block operation is composed of several rounds of substitution and permutation. The diagram shows the operations for an AES encryption using a 128-bit key. Successive blocks can be chained following several operating modes described in next slides.
As for DES operations, Electronic codebook (ECB) and Cipher Block Chaining (CBC) are supported. ECB can be used safely for small messages only (a few blocks). In CBC mode, the output of the first operation is injected at the input of the next block operation as described in the diagram. For the first round, an initialization vector is required.

The third mode of operation is the Counter Mode, or CTR. In this mode, the AES engine is used as a random stream generator. The resulting random stream is mixed with the input message with an exclusive-Or operation. As for CBC, CTR requires an initialization vector different for each encryption session.
The two modes of operation mentioned in this slide add authentication and integrity to confidentiality.

The authentication mechanism is applied both on the payload message that will be encrypted and also on additional data that requires only authentication. This last part is called the header.

First mode is the “Counter with CBC-Message Authentication Code”, or CCM. This mode combines a first pass of AES-CBC mode for authentication tag computation (MAC). The MAC is then encrypted with the payload in a second AES-CTR pass. The same key is used for both the CTR and CBC passes.

Second authenticated encryption mode is the Galois counter mode, or GCM. Confidentiality of data is provided using a CTR mode and
authenticity of the confidential data is provided using a universal hash function that is defined over a binary Galois field.

GCM is faster than CCM as it requires only one pass of the AES engine for each payload block. Furthermore, the payload message can be processed on-the-fly without storing it for multi-pass processing.
The cryptographic processor complies with the Data Encryption Standard and the Advanced Encryption Standard. These standards are published under Federal Information Processing Standards publications.
Processing times are given for block operations. DES and Triple DES operations are based on a 64-bit block while AES is based on a 128-bit block.

Triple-DES requires obviously three times more processing than a simple DES.

AES times are presented in the table. For large messages of several 128-bits payload blocks, we can see that GCM is more efficient than CCM.
The cryptographic processor block diagram is presented in the slide. The peripheral is composed of several hardware modules:
- the processor core responsible for one AES or DES block operations,
- input and output FIFOs connected to the bus interconnect,
- and a module that embeds control and status registers.
Two functional interrupts are defined for the peripheral: One set when the input FIFO is ready to receive data and one set when output data are ready to be flushed by the CPU or the DMA.

The DMA has two streams plugged to the cryptographic processor. These two streams share the same channel (#2); output stream has higher priority than the input one.
Here is an overview of the status of the cryptographic processor in each of the low-power modes. Cryptographic operations are not possible when the device is in Stop and Standby modes.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run</td>
<td>Active.</td>
</tr>
<tr>
<td>Sleep</td>
<td>Active. Peripheral interrupts cause the device to exit Sleep mode.</td>
</tr>
<tr>
<td>Stop</td>
<td>Frozen. Peripheral registers content is kept.</td>
</tr>
<tr>
<td>Standby</td>
<td>Powered-down. The peripheral must be reinitialized after exiting Standby mode.</td>
</tr>
</tbody>
</table>
This is a list of peripherals related to the cryptographic processor.
Refer to the DMA training for more information about the cryptographic channel configuration.
And please refer to the hash trainings if you want to go further on cryptographic engines.
For more details and additional information, refer to the following:

- Application notes AN4023 & AN4024: STM32 Secure Firmware Update (SFU)
- User manual UM0586: STM32 Cryptographic Library

For more details, please refer to these documents available on our website.