AES-IP Design Guide

Rev1.00 28-Feb-2023

1 AES : Advanced Encryption Standard IP core

AES implement the advanced encryption standard (AES) algorithm in ECB mode which is suitable for modifying to another mode of operation that requires high throughput. It is widely used in many applications like file encryption, processor security, and secure file transfer protocol to provide data confidentiality which usually works with authentication functions. AES series consist of 3 IP-core, AES256 Super-Speed (AES256-SS), AES256 and AES128. For more information about AES IP specification and reference design, please check https://dgway.com/ASIP_E.html#AES.

As shown in Figure 1.1, AES256-SS is used as the base for implementing AES256-CTR in SSH authenticated encryption scheme. It is used in conjunction with an authentication function, such as HMAC-SHA-1. After deriving encryption and authentication keys, initial IV concatenated with counter and encryption key are used as inputs for AES256-SS to operate in CTR mode. After 15-clock of key setting, AES256-SS can encrypt/decrypt 128-bit data every clock.

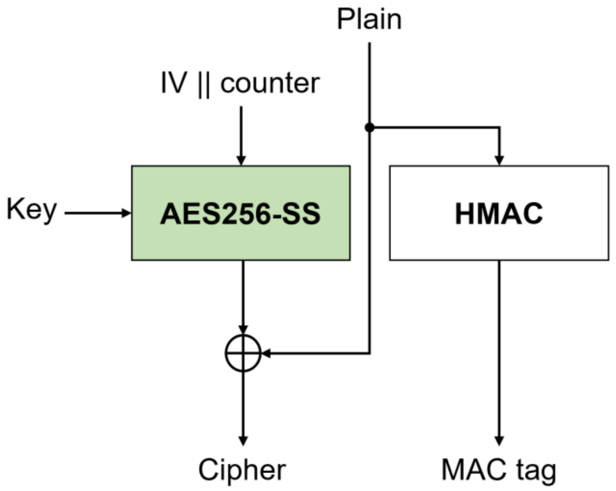

Figure 1.1 AES256-SS in SSH authenticated encryption scheme.

Figure 1.2 shows that AES256 is implemented as the base for AES256-CBC in the IPsec authenticated encryption scheme. AES256 can support XOR operation between plain payload and the previous cipher block before encryption, which makes the encryption of each block dependent on the previous block. AES256IP can be combined with HMAC to provide authentication.

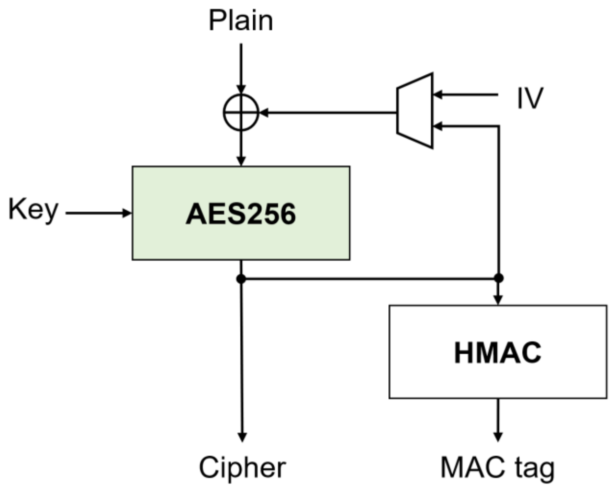

Figure 1.2 AES256 in IPsec authenticated encryption scheme.

2 AES-XTS : Encryption IP core for data storage

AES256-XTS implement the 256-bit key advanced encryption standard with XEX Tweakable Block Cipher and Ciphertext Stealing (XTS). It is widely used in protecting the confidentiality of data on storage devices. According to ciphertext stealing method, it can encrypt or decrypt sequences of arbitrary lengths of data blocks where the data length must be more than or equal 128 bits or 16 bytes. For more information about AES-XTS IP specification and reference design, please check https://dgway.com/ASIP_E.html#AESXTS.

Figure 2.1 shows the example system for writing plain data to storage and reading plain data from storage. In case storing sensitive data, the encryption process is required to protect the data from unauthorized access by encrypting plain data before writing to the storage and decrypting the cipher to access the data.

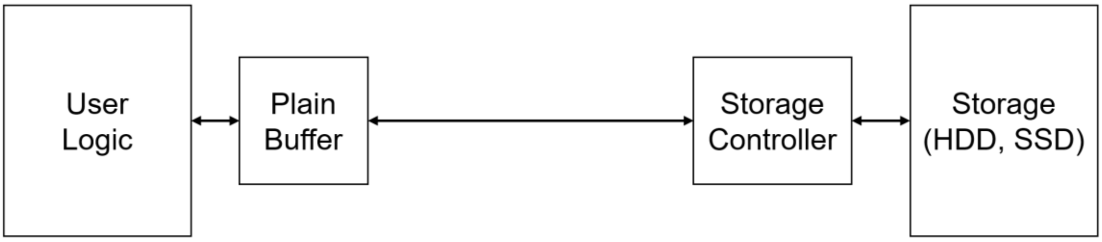

Figure 2.1 unsecure system for writing/reading data from storage

As shown in Figure 2.2, AES256-XTS can be implemented to encrypt and decrypt confidential data that transfer between user buffer and storage. The sector number or Logical Block Address (LBA) is used with a key to derive IV as the input of AES256-XTS. After adding security with AES256-XTS IP, users can access plain data in the same way as unsecure system.

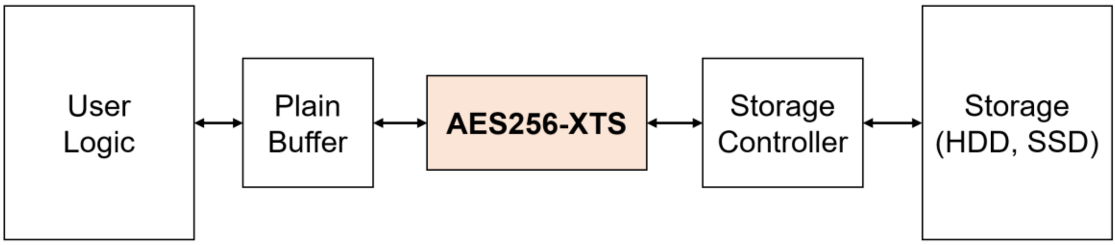

Figure 2.2 secure system for writing/reading data from storage

3 AES-GCM : Encryption IP core for Communication

AES256-GCM IP Core implement the advanced encryption standard with 256-bit key in Galois/Counter Mode (GCM) which is widely used for Authenticated Encryption with Associated Data (AEAD) application, including MACSEC and TLS (Transport Layer Security) versions 1.2 and 1.3. It works with 256-bit AES-key and 96-bit Initialization Vector and supports zero-length plaintext/ciphertext input which is the special case of GCM mode, called GMAC, and also support zero-length AAD.

AES256-GCM series consist of 3 IP-core, AES256GCM1GIP, AES256GCM10G/25GGIP and AES256GCM100GIP. Its version is selected to match user's system by considering application throughput such as AES256GCM100 IP can be used effectively on 100G Ethernet. For more information about AES-GCM IP specification and reference design, please check https://dgway.com/ASIP_E.html#AESGCM.

Figure 3.1 shows the example client's system to communicate with the server. The plain data is transferred through the network which Man-in-the-middle can access, intercept and modify data. To protect transferring data, key exchange, handshaking and encryption/decryption processes are implemented with TLS on top of TCP/IP layer. As shown in Figure 3.2, AES256-GCM is used as a core module in TLS to encrypt/decrypt application data working with x25519 and HKDF to derive key and iv and RSA to verify server certificate and signature.

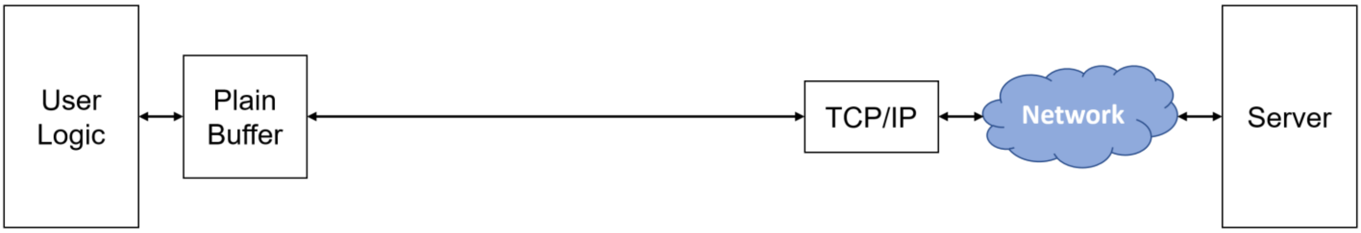

Figure 3.1 unsecure system to communicate with the server

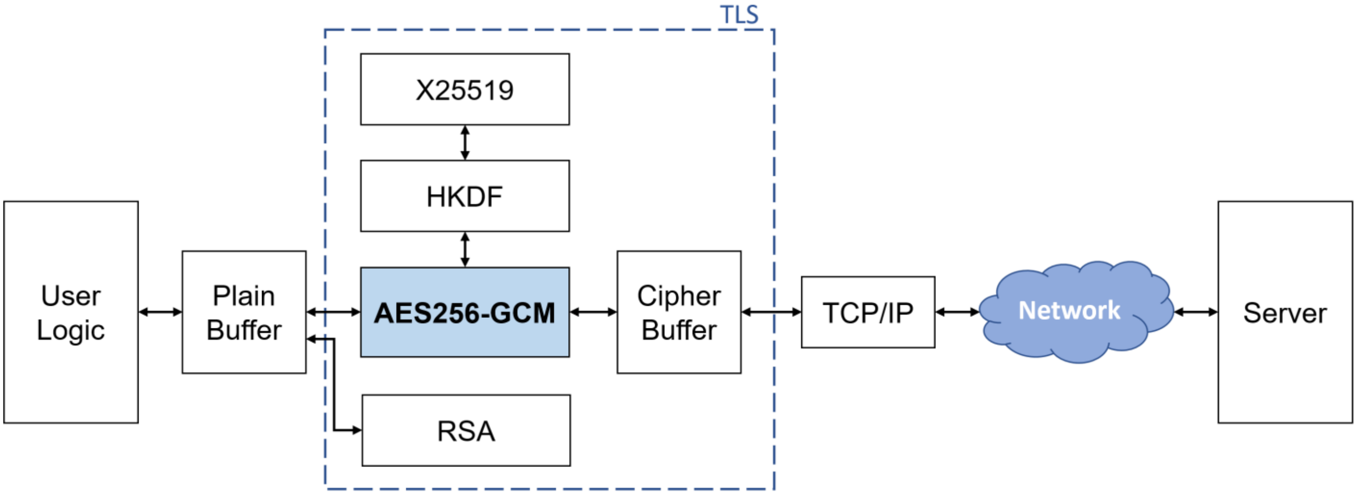

Figure 3.2 secure system with TLS to communicate with the server

4 Revision History

Revision	Date	Description
1.00	28-Feb-2023	Initial version release