Key Size for 25G-EPON and 50G-EPON

Glen Kramer, Broadcom

Only one question

- **Should the 1904.4 support only 128-bit keys, only 256-bit keys, or both 128-bit and 256-bit keys?**

- **How to answer:**
  1. Complexity impact of supporting one key size versus two key sizes
  2. Cryptographic strength
  3. ~~Performance impact~~
  4. Key sizes currently required by other relevant standards
  5. Any external constraints operators may have within their COs
  6. Design impact:
     1. Key memory
        Number of keys per OLT ASIC =
        #Ports/chip × (#ONUs/Port + #multicast_LLIDs/port) × 2 keys/sec. association
     2. Latency
     3. Power

Review of the Advanced Encryption Standard

- FIPS 197 provides three variants of AES, each with a different key size: 128, 192, and 256 bits. The 192-bit and 256-bit variants not only have larger key sizes but also require additional iterations of the AES round function — 12 and 14 rounds, respectively — compared to 10 rounds for the 128-bit variant. It is reasonable to expect that the 192-bit and 256-bit variants will always require significantly more computations to attack than the 128-bit variant and may, therefore, provide alternatives in case of significant advances in computing power or cryptanalysis. Currently, however, all three keys sizes are considered secure, and it seems that this will continue to be the case for the foreseeable future.

NISTIR 8319, July 2021

FIPS 197 update

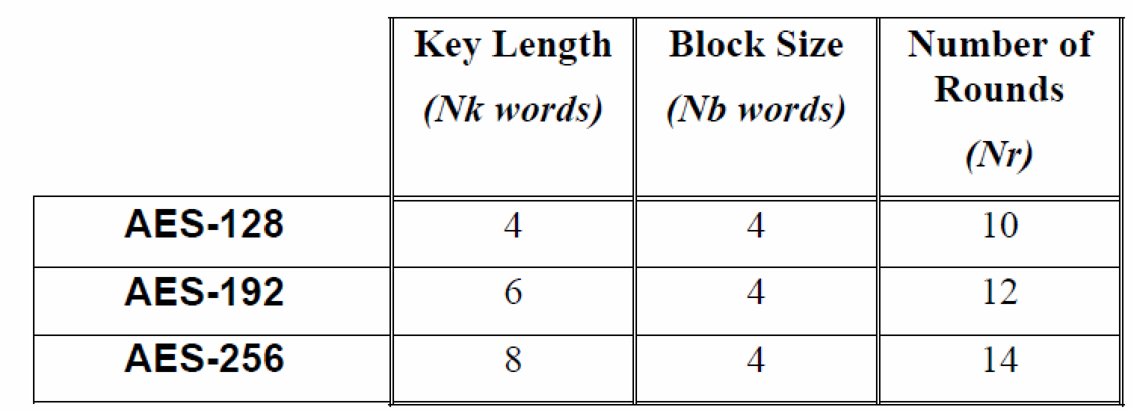
Rationale for Updating FIPS 197

- The technical content is the specification of a family of three block ciphers: AES-128, AES-192, and AES-256, where the numerical suffix indicates the bit length of the key. Since AES is adopted widely, the main question for the review is whether the specified block cipher family is sufficiently secure. The following is a summary of the security assessment:
  - **Classical security** [Sections 3.1 and 3.2 of NISTIR 8319]: <u>The key sizes remain adequate against classical exhaustive search</u>. For the classical analytic attacks on instances of the AES algorithm that are listed in Table 2 of NISTIR 8319, either 1) the attack only applies to an unapproved, weakened variant, in which the number of rounds is reduced by at least three; or 2) the computational complexity of the attack is prohibitive. In the second category, the largest theoretical reduction in computational complexity over generic, exhaustive search occurs under the restrictive assumption of related-keys, and only for AES-192 and AES-256.
  - **Key Size and Post-Quantum Security** [Section 3.3 of NISTIR 8319]: If large-scale quantum computers are developed, Grover's algorithm would facilitate a brute force search for the key with computational work that is roughly the square root of the classical computational work. NIST expects to issue appropriate guidance on parameter choices and post-quantum security as part of the Post-Quantum Cryptography project.

Performance Impact

A Comparative Study on AES 128 bit and AES 256 bit. International Journal Of Computer Sciences And Engineering. Vol 6. 30-33, 2018

- ❑ Larger key requires more key expansion rounds
- ❑ But the performance hit shown in this paper seems excessive
  - **This may not be relevant to silicon implementations. Encryption will always run at line rate. May require deeper pipeline (negligible impact on latency and power).**



	Key Length *(Nk words)*	Block Size *(Nb words)*	Number of Rounds *(Nr)*
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Figure 4. Key-Block-Round Combinations.

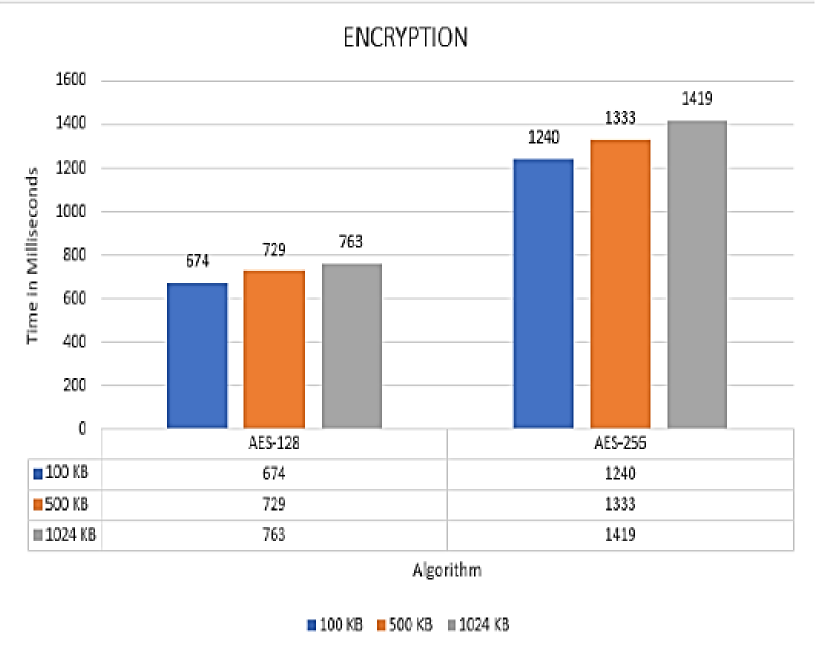


Figure 3. Comparative encryption time of AES-128 and AES-256

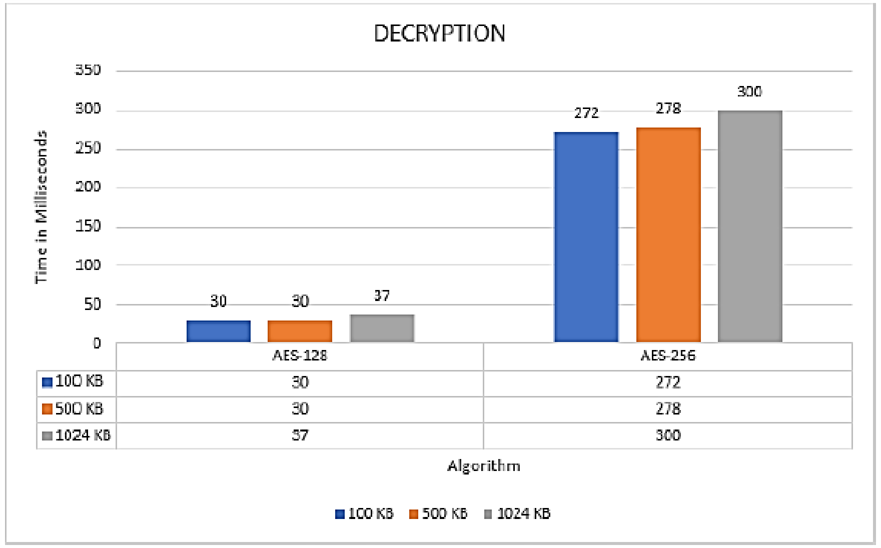


Figure 4. Comparative decryption time of AES-128 and AES-256

Key sizes required by other standards

- MACSec
  - This standard uses a KDF that is compatible with the counter mode KDF described in the NIST Special Publication 800-108. The KDF uses a pseudorandom function (PRF) which shall be AES-CMAC-128 when the derivation key is 128 bits, and AES-CMAC-256 when the derivation key is 256 bits.
- ITU-T G.9804.2
  - The default algorithm used for XGEM payload encryption is the AES-128 [NIST FIPS-197] cipher, used in Counter mode (AES-CTR), as described in [NIST SP800-38A]. Cipher algorithms AES-128 (mandatory), AES-256 (mandatory), Camellia-128, Camellia-256, and SM4(-128) [ISO/IEC 18033-3:2010] can be configured via the OMCI, as defined in clause 9.1.2 [ITU-T G.988]. The configured cipher algorithm is used for both upstream and downstream, unicast and multicast.
  - The default cipher is the advanced encryption standard (AES) encryption algorithm [NIST FIPS-197] with 128 bit key length. The use of additional ciphers (both algorithm and key length) can be configured via the OMCI. Before OMCI configuration occurs, the default cipher will be used.

Additional considerations

- Most PON silicon supports multiple generations of PON and multiple flavors (IEEE, ITU-T).
- AES-128 is the default in ITU-T G.9804.2 and in DPoE 2.0 (and SIEPON Package A, by reference). The new chips are likely to support AES-128 if they support previous generation of PON

Straw Poll

□ I prefer the following encryption key sizes for IEEE 1904.4 (vote for one only)

1. Only 128-bit key shall be specified ______

2. Only 256-bit key shall be specified ______

3. 128-bit and 256-bit keys are
   mandatory to support;
   operator selects the key size to use______

Thank you