IEEE P802.11
Wireless LANs

|  |
| --- |
| New Comment Resolution for CID 7093 |
| Date: 2024-06-20 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Ali Raissinia | Qualcomm Inc. |  |  | alirezar@qti.qualcomm.com |
|  |  |  |  |  |

Abstract

This document provides a new resolution for CID 7093.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 7093 | Kneckt, Jarkko | 6072.00 | 13 | J.14 | The order of "Output block [n]" values in the table is misleading. Based on Figure 11-65 and Figure 11-66, Octet 15 is actually the first output from AES 128 block corresponding to M\_0,0, but the table seems to imply that Octet 0 is the first value. The output ordering must be 100% clear in order to ensure interoperability, since it is critical for the definition of the IEEE 802.11az Secure LTF | Update the Table in Appendix J.14 to reflect that Octet 15 for "Output block [n]" is the first output of the AES 128 block for secure LTF generation. Specifically make the following changes: move "Output block [0]" and "Output block [1]" to the end of table, so that it has a separate header, where the header will have the following values from left to right: Mi,15, Mi,14, ..., Mi,0. The mapping between new header label and existing header label should be as follows: 1st row: M0,15 = Octet 0 = aa, M0,14 = Octet 1= f6, .... M0,0 = Octet 15 = f1, and 2nd row: M1,15 = Octet 0 = 54, M1,14 = Octet 1 = 15, .... M1,0 = Octet 15 = 5a to reflect the output stream in Figure 11-65 and Figure 11-66. Last clarification is to update "Output block [0]" to "Output block [i=0]" and update "Output block [1]" to "Output block [i=1]". This new table would clearly specify the output from the AES 128 block and ensure interoperability between devices | ACCEPTED (PHY: 2024-03-12 23:02:16Z)REVme Editor: The resolution in the document overwrites all changes that were approved in the motion on March 14, 2024<https://mentor.ieee.org/802.11/dcn/24/11-24-xxxx-00-00m-new-comment-resolution-for-cid-7093.docx>  |

**Discussion**: Agree with the commenter however it would be better to also clarify octet ordering for IV and LTF Key in Figure 11-65 and 11-66 plus additional info regarding the psueorandome phase rotation octets as wells as QAM 64 symbol octets in Table in J.14

Resolution for CID 7093

*Note to Editor: This resolution overwrites all changes that were approved in the motion on March 14, 2024.*

*TGm editor: Change Figure 11-65 as shown below:*



*TGme editor: Change Figure 11-66 as shown below:*



*TGme editor, replace the table in J.14 with table below:*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Octet** | **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| **LTF\_KEY** | d2 | a8 | a2 | b7 | 6c | 3c | 29 | 2d | 81 | e1 | 82 | a4 | 69 | fd | e8 | 3c |
| **LTF\_IV** | 00 | 10 | 18 | 32 | 76 | 54 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 |
| **AES counter [0]** | 00 | 10 | 18 | 32 | 76 | 54 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 |
| **Output block [0]** | M0,15 | M0,14 | M0.13 | M0.12 | M0,11 | M0,10 | M0,9 | M0,8 | M0,7 | M0,6 | M0,5 | M0,4 | M0,3 | M0,2 | M0,1 | M0,0 |
| aa | f6 | 2c | 30 | 6b | cd | 8a | 5d | 89 | 80 | 8b | 03 | 8e | da | 43 | f1 |
| (I,Q)=(2,5) | (I,Q)=(3,3) | (I,Q)=(1,5) | (I,Q)=(0,3) | (I,Q)=(6,5) | (I,Q)=(5,4) | (I,Q)=(2,4) | (I,Q)=(5,6) | (I,Q)=(4,4) | K=1 | K=1 | K=0 | K=1 | K=3 | K=2 | K=7 |
| **AES counter [1]** | 00 | 10 | 18 | 32 | 76 | 54 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 01 |
| **Output block [1]** | M1,15 | M1,14 | M1.13 | M1.12 | M1,11 | M1,10 | M1,9 | M1,8 | M1,7 | M1,6 | M1,5 | M1,4 | M1,3 | M1,2 | M1,1 | M1,0 |
| 54 | 15 | f0 | 5c | 7f | c7 | ee | f5 | 9b | c4 | 58 | d2 | f4 | 6b | 5b | 5a |
| (I,Q)=(1,2) | (I,Q)=(5,2) | (I,Q)=(0,3) | (I,Q)=(1,6) | (I,Q)=(7,7) | (I,Q)=(7,0) | (I,Q)=(3,5) | (I,Q)=(5,3) | (I,Q)=(6,6) | (I,Q)=(1,0) | (I,Q)=(0,6) | (I,Q)=(2,2) | (I,Q)=(1,3) | (I,Q)=(6,5) | (I,Q)=(6,6) | (I,Q)=(2,6) |
| **…****(I, Q) = input index for 64-QAM octet, I = input bits (B0 B1 B2), Q = input bits (B3 B4 B5) defined in Table 17-18.****The integer k is defined in Equation (27-131) that is used to construct the pseudorandom phase rotation.+ P** |

**References: P802.11REVmeD5.0**