# Public Comments on the April, 2006 Draft of Special Publication 800-38D

This document contains the comments that NIST received during the 45-day period of public comments on the Draft Special Publication 800-38D: *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication*.

# Bruno Couillard

**BC5 Technologies' Comments on the following document:**
**"NIST Special Publication 800-38D"**
**DRAFT Version Issued April 2006**

## Introduction:

The comments provided on the subject document are divided into three (3) categories: Critical, Substantive, and Administrative. Critical comments are comments that are deemed to require resolution before completion of this document. Substantive comments are comments that improve technical accuracy or clarify an item. Administrative comments correct items such as punctuation, grammar and spelling.

## Critical Comments

| Number | Reference | Comment |
|---|---|---|
| 1. | | |

## Substantive Comments

| Number | Reference | Comment |
|---|---|---|
| 1. | Section 3, 2nd paragraph, first bullet | Would suggest replacing "online" by "in-line". |
| 2. | Section 4.2.1 | Add the following:<br>"A Additional Authentication Data" to the list. |
| 3. | Section 5.2.1, 3rd paragraph. | Would suggest removing the first sentence since it seems to be restated differently in the second sentence of the same paragraph. |
| 4. | Section 3, 1st paragraph | Would suggest changing "$11100001 0^{120}$" to<br>"$11100001 \| 0^{120}$" |
| 5. | Section 8.1, Algorithm 4, Steps | In step 2.a, would suggest replacing "$J_0 = IV \| 0^{31}1$." to<br>"$J_0 = IV \| 0^{31} \| 1$." |

## Administrative Comments

| Number | Reference | Comment |
|---|---|---|
| 1. | Section 7.2, 1st paragraph | Change the bracket used in the equation from "$\lfloor$" and "$\rfloor$" to "[" and "]". |
| 2. | Section 8.1, 4th paragraph | In the third sentence, correct the word "function". |

## Matt Ball

There is an issue that just came to light about the GCM mode, concerning compatibility between the proposal from McGrew and Viega, and the NIST draft SP 800-38D. It looks like the GHASH functions are incompatible when used to process an IV that is not 96-bits long. The original GCM proposal includes the IV length within the GHASH calculation, and the new NIST proposal does not include this length.

This difference invalidates the GCM test vectors 10 and 11 within P1619.1-D7, and also invalidates any existing GCM implementation that supports an IV that is not 96-bits long. Was this the intent of SP 800-38D, or should we expect the final NIST standard to match the GCM proposal?

Here are more details:

In the GCM proposal by McGrew and Viega, the variable Y0 is computed using GHASH(H, {}, IV) (see equation (1), page 5). Within equation (2), the bit-length of the IV is included at the end of the computation.

In Draft SP 800-38D, the GHASH function specified in 7.4 does not include a length field. This is okay for authenticating the data because step 5 of section 8.1 then includes "len(A) || len(C)" at the end. However, the J0 computation does not include the length.

I believe that it would be possible to make SP 800-38D match the GCM proposal by making the following change to SP 800-38D, section 8.1 "Authenticated Encryption" (changes in **bold**):

Steps:
...
2. Define a block, J0, as follows:
...
b. If len(IV) <> 96, then
J0 = GHASHh(IV || 0^s || **0^64 || [len(IV)]64**)

where '^' is the exponentiation operator (which in this case is actually a duplication operator).

Thanks!

Matt Ball
Embedded Software Engineer
Quantum Corporation
4001 Discovery Drive, Suite 1100
Boulder, CO 80303
(720) 406-5766

---

[received subsequently]

... While I'm at it, I had another quick comment on SP 800-38D:

In section 5.2.1, I suspect that the limits for the bit lengths should be as follows:

len(A) <= 2^64 - 1
1 <= len(IV) <= 2^64 - 1

Since the bit-length of the A and IV fields is encoded within a 64-bit integer, the largest possible value is 2^64-1.

## Wan-Teh Chang

I am a software engineer working on the NSS crypto libraries(http://www.mozilla.org/projects/security/pki/nss/), so I reviewed Draft Special Publication 800-38D from the point of view of an implementor. Overall the Draft is well written that I believe I can implement GCM to it. Below are my comments and suggested changes. Almost all my suggested changes fix minor typos or ambiguities that I believe a competent implementor can correct for themselves.

1. Page 1, in Sec. 3, we have "(FIPS) Pub. 197 [2]".

It is more common to use "PUB" instead of "Pub." in the name of a FIPS Publication.

2. Page 3, in Sec. 4.1, the definition of "Block"

Perhaps it should say "For a given block cipher and key", as in the definition of "Block Size"?

3. Page 3, in Sec. 4.1, the definition of "Block Cipher" says "A parameterized family of permutations". This is a very mathematical way to define "Cipher". I suggest that it should at least say the parameter is the key.

4. Page 4, in Sec. 4.1, the definition of "Mode of Operation (Mode)" is not clear. Perhaps we can change "features" to "is based on" or "uses ... as a component/building block".

5. Page 4, in Sec. 4.2, it would be good to add

ICB The initial counter block

6. Page 5, at the end of Sec. 4.2, in the X*Y item, it might be good to explain that this document also uses * to denote integer multiplication, for example, in Sections 8.1 and 8.2 in the definitions of s, u, and v.

7. Page 6, in the last paragraph of Sec. 5.1, "the parties to the information" probably should be "the parties of the communication" or "the parties in the communication".

8. Page 6, in Sec. 5.2.1, I'm curious as to how the limit on len(P), 2^39 - 256, was determined. That limit is only 64 GB, which isn't that big today. There are 500 GB hard drives for desktop computers. So the document probably should point out that the algorithm can't be applied to files/messages larger than 64 GB.

9. Page 6, in Sec. 5.2.1, len(A) cannot be equal to 264, otherwise it can't be expressed as a 64-bit string ([len(A)] sub 64) in Sections 8.1 and 8.2 (Algorithm 4 Step 5 and Algorithm 5 Step 6).

10. Page 10, in Sec. 7.3, Step 3, LSB(Vi) should be written as LSB sub 1(Vi) because the LSB function is defined with a subscript s in Sections 4.2 and 7.1.

11. Page 10, in Sec. 7.3, the last paragraph says "if u denotes the indeterminate". It may be better to use "variable" instead of "indeterminate".

Also in that paragraph, the last sentence has "R || 1", which is 129-bit long, or equivalently, corresponds to a polynomial of degree 128. I just wanted to make sure that's correct.

12. Page 10, in Sec. 7.4, the underline for "Algorithm 2: GHASH sub H (X)" is broken under the subscript H. This is a very minor cosmetic problem. This problem is also in other sections whose algorithms' notations have a subscript.

13. Page 12, in Sec. 7.5, "only the rightmost string in the sequence": change "string" to "block".

14. Page 13, in Sec. 8.1, we have "the minimum number of '0 bits", where I use ' to denote the opening single quote. The opening single quote before 0 should be removed.

There are three other instances of this problem: one in Sec. 8.1 and two in Sec. 8.2.

15. Page 17, in Appendix A, we have:

if n denotes the total number of blocks in the encoding (denoted S in Secs. 8.1 and 8.2 above) of the ciphertext and AAD, ...

Since S (the output of the GHASH function) is one block long, the above sentence isn't right. I don't know how to fix this. Perhaps the following?

if n denotes the total number of blocks in the encoding (the input to the GHASH function in the definition of S in Secs. 8.1 and 8.2 above) of the ciphertext and AAD, ...

16. Page 18, in Appendix B, we have "a sequential message number, or a timestamp". That comma can be deleted.

17. Page 19, in Appendix C, I suggest using the full name "National Institute of Standards and Technology" instead of the abbreviation "Natl. Inst. Stand. Technol.", or just use "NIST".

18. It may be good to explain why GCM is better than the counter mode plus HMAC.

Wan-Teh Chang
Software Engineer
Red Hat