Public Comments on the Draft SP 800-38G

On July 8, 2013, NIST announced a period of public comment, ending September 3, 2013, on Draft Special Publication 800-38G, which specifies three modes of the AES block cipher for format preserving encryption. The announcement was posted on the News and Events page at NIST's Computer Security Resource Center.

NIST received the following public comments:

Wayne Nugwin

Greetings,

Per my review of the SP 800-38G draft and as stated in the Introduction of section 3, "FPE has emerged as a useful cryptographic tool, whose applications include financial-information security, data sanitization, and transparent encryption of fields in legacy databases." However, employing FPE for data sanitization is not further discussed in this publication.

Please consider developing and further addressing how FPE can be employed for data sanitization (and encryption of fields in legacy databases), as it may be of interest and possibly applicable to BLS information and systems.

Thank you.

Wayne Nugwin
Bureau of Labor Statistics
Division of Network & Information Assurance

Tim Masey

To the Computer Security Division of NIST,

I have implemented and run a Format Preserving Encryption product for over 3 years at AAA AutoClub Group, based in Dearborn Michigan. The benefits are tremendous for application integration without need of specific database modifications or changes. This has allowed our application development teams to improve security by protecting critical information with minimal to none application changes and insert encryption technology into the application flow. The goal of preserving format is to ensure that protection is maintained at a high level and fit the application requirements without re-architecting a system. Format Preserving technology such as described in NIST 800-38G, accomplishes this objective with acceptable algothrimic principles for protection of data. My recommendation is that the standard be ratified.

If there are any questions related to this recommendation, please respond via email.

Sincerely,

Tim Masey
Director of Enterprise Information Security
AAA - The Auto Club Group

Steve Kozman

Hello:

I am supportive of the standard and agree that it's a useful cryptographic tool. Generally, when you encrypt data and change its format, there's often some part of your IT environment that is unable to handle the encrypted data. Finding and fixing these problems is expensive and time-consuming. The approaches described in the draft of SP 800-38G make integrating encryption into these environments much cheaper and easier, and that means that more sensitive data will get protected.

Thanks

Michael Cheaney

The benefits of format preserving encryption have a huge cost benefit to the industry beyond the security of the encryption strength itself. Plaintext to cipher text length preservation not only meets storage space concerns from a volume perspective, but it allows for zero changes in the storage of data in column scenarios which is extremely important in the z/OS world and many legacy applications that now require encryption.

From a data leakage perspective, format preserved data allows for outbound scanning tools to recognize PII or PCI data is leaving the company without needing the keys to actually decrypt the data. It does introduce false positives if the valid business event wasn't already on an exceptions list, but those events should be accounted for so that any sensitive data leaving the company is known.

Statistics programs can also remain unmodified in regular expressions to gather information about the data without ever knowing what the actual values are, but understanding what they are. (Ex. SSN, Credit Card, email addresses, and street addresses)

FPE may not be the best solution for encrypting all data, but its value is easily seen in just the 3 simple scenarios I mentioned.

Thank you,

Michael Cheaney
Principal Member of Technical Staff

Travis Spann

Dear NIST.
Thanks for the opportunity to comment on SP800-38 G:

· Please include example vectors (known inputs and known outputs) within the special publication in support of testing and debugging implementations of this new mode.

· There is a limited number of shall statements in this special publication. What criteria will be used for vendor affirmation of conformance to this recommendation before such a time as CAVP includes this mode in the CAVS testing tool?

· Please fix the following: "**Error! Reference source not found."**

Sincerely,

Travis Spann | ÆGISOLVE, INC. | President, Laboratory Director

Robert Burns

NIST,

Attached you will find Thales e-Security's consolidated comments regarding the proposed NIST SP800-38G standard.

Generally speaking, Thales e-Security is in support of NIST's efforts to standardize FPE modes of encryption, but we have significant reservations about standardizing on modes which appear to be encumbered with financial obligations and/or licensing restrictions. Publishing a standard which financially benefits a commercial entity seems to run counter to the spirit of standardized cryptography as promoted by NIST.

If you require any additional information or clarification on our comments, please feel free to contact me at the email address and/or phone number below.

Thanks,

Bob

CLASSIFICATION : Thales e-Security OPEN

Robert Burns
Security Principal
Office of the CTO
THALES Information Systems Security

1	2	3	4	5	6	7	8
Com-ment #	**Organization Name**	**Chapter/ Subsection Appendix** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[1]	**Comment (justification for change)**	**Proposed change**	**Resolution on comment**
1.	Thales e-Security	General	N/A	ge	Although we are very supportive of having FPE cipher modes standardized by NIST and adopted across the industry as standard mechanisms for data protection, we have significant reservations about the IP claims being made which impact all proposed implementations. Despite the offer of non-discriminatory licensing, we are opposed to NIST standards which are encumbered with licensing restrictions and/or costs. We believe this runs counter to the goal of having national standards.	A) Negotiate a more liberal, cost free license for the use of all modes in the current draft specification. B) If (A) is not possible, then replace existing modes with ones which are not encumbered with IP issues. C) If neither (A) or (B) possible, we recommend withdrawing the SP800-38G draft from publication consideration.	
2.	Thales e-Security	4.4	Page 7, Paragraph 7	ed	The paragraph begins with "Given a byte string X,…". We believe this should be a bit string.	Change paragraph to begin as, "Given a bit string X, the length of X in bytes is…"	
3.	Thales e-Security	5.4	Paragraph 4 and Figure 1	ed	Given that footnote 4 indicates that '+' is any reversible function which preserves the length of the string, it is possible that the use of the '+' could potentially be confusing.	Suggest replacing the overloaded '+' character with another symbol, or function (e.g. MODADD(a, b)) to remove ambiguities. Updates would be required to section 4.3, as well as on page 15: "indicated by the "+" operation.)	
4.	Thales e-Security	5.5	Page 12, Paragraph 1	ed	The sentence contains an errant ')' character.	Remove redundant ')' character so the sentence reads, "The function REV(X) – defined…"	
5.	Thales e-Security	5.5	Page 12, Paragraph 2	ed	The referenced PRF function is also utilized in FF2.Encrypt and FF2.Decrypt.	Update the paragraph to indicate that this PRF is also utilized in the FF2.Encrypt and FF2.Decrypt functions.	
6.	Thales e-Security	5.5	Page 13, Algorithm 3: REV(X), Step 2	ed	The other algorithms reference arrays from element 1-len(x), whereas Step 2 here is referencing the Y array as a zero-indexed element. This error will return an indeterminate byte (e.g. Y[0] not assigned) and will truncate the return by not returning Y[LEN(X)].	Change Y referencing to be consistent with the other algorithms.	
7.	Thales e-Security	Appendix A	Paragraph 3	te	Although the cited reference (Appendix H of [1]) provides some justification for choosing a fixed number of rounds, the reference emphasizes that "these values are minimums, not recommended values". Furthermore, this specification chooses	Recommendations: A) Provide additional justification for the choice of rounds for each mode to explicitly state the trade-offs	

1	2	3	4	5	6	7	8
Com-ment #	**Organization Name**	**Chapter/ Subsection Appendix** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[1]	**Comment (justification for change)**	**Proposed change**	**Resolution on comment**
					10 for FF1, 10 for FF2 and 8 for FF3 without any justification or background as to why 10 is required for two modes, yet 8 is sufficient for FF3.	considered between security and performance. B) Consider increasing the rounds to include sufficient 'future proofing'. Having only two additional rounds above the 'minimum' for FF1 and FF2 seem an insufficient buffer, while leaving FF3 at the minimum seems problematic. C) Consider normalizing the rounds to be consistent across all modes to avoid potential confusion and implementation issues. Normalization should favour higher values (e.g. 10), although we would recommend consideration of higher values with more margin (e.g. 14).	
8.	Thales e-Security	6.1	Paragraph 1	te	The specification for FF1 mentions that the tweak is optional. Given the intended application of this technology (i.e. encrypting small pieces of data) and the significant security enhancements that they can provide (reference FFX[radix] Appendix F), it seems counter intuitive to allow misuse of the mode by making the tweaks optional.	Make the tweaks required and set minimum lengths.	
9.	Thales e-Security	6.1	Page 15, Paragraph 2	ed	Missing reference.	Fix reference.	
10.	Thales e-Security	6.2	Paragraph 1	te	The specification for FF2 mentions that the tweak is optional. Given the intended application of this technology (i.e. encrypting small pieces of data) and the significant security enhancements that they can provide (reference FFX[radix] Appendix F), it seems counter intuitive to allow misuse of the mode by making the tweaks optional.	Make the tweaks required and set minimum lengths.	
11.	Thales e-Security	6.2	Page 17, Last Paragraph	ed	Missing reference.	Fix reference.	
12.	Thales	7	All	ed	This section makes no mention regarding the requirement that the supported cipher is required to be NIST approved.	Consider adding a sentence regarding the requirement to utilize a NIST approved cipher.	

1	2	3	4	5	6	7	8
Com-ment #	**Organization Name**	**Chapter/ Subsection Appendix** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[1]	**Comment (justification for change)**	**Proposed change**	**Resolution on comment**
	e-Security						
13.	Thales e-Security	7	Paragraph 4	ed	Although subtle, the phrase "support a common value for the base" does not actually make two implementations interoperable. Both implementation may be perfectly compatible and support common values, but unless they are both USING the same base they will not interoperate. Same comment for the tweak as well.	Recommend the alternative phrasing: "Two implementations can only interoperate when they use the same value for the base. Similarly, two implementations of FF2 can only interoperate when they also use the same value for the tweak base."	

Eric Lengvenis

To whom it may concern,

I would like to offer a statement of support for the effort to standardize the three format-preserving modes of operation in the current draft of SP 800-38G and to make a few minor comments. As a large financial institution we have a preference for technology in conformance with standards put out by NIST and ASC X9. These help guarantee a level of confidence in the implementation of encryption technology. To this end, we have been working with X9 to standardize FPE in X9.124, but this would be even more valuable as NIST standards if the validation of the modes is incorporated into the FIPS 140 validation program. If this comes to be, our HSM vendors could incorporate FPE into FIPS-compliant appliances which is very desirable. Already FPE is widely-used but not defined in a standard which creates tension between using the technology that allows us to encrypt in legacy applications which cannot be overhauled to allow for the format changes required by other approaches and our preference for standardized technology. For these reasons, I support this effort.

On to the comments. There are two source errors in the document; one on page 15 and the other on page 17. Both appear to be referencing the Feistel diagram, but the link is incorrect. The other, is a question -- why is not the full BPS approved, but the specific subset is? I think it would merit a statement as to why, given that the proposed mode defines it.

Thank you,

Eric Lengvenis
Information Security Architect
Vice President
Enterprise Information Security Architecture (EISA)

Andrew Price

We fully support moving forward with the publication of SP 800-38G. The format-preserving encryption technologies that it specifies are an important tool for protecting sensitive information in complex IT environments, and their availability can make the difference between sensitive data being encrypted and sensitive data not being encrypted. It's hard to get an accurate estimate of the economic losses caused by data breaches, but it's certain that these losses can be greatly reduced by the more widespread use of encryption. And because the technologies defined by SP 800-38G make this practical when it would not be practical with existing encryption approaches, making these technologies acceptable for broad use is definitely a step in the right direction.

Regards,

Andrew Price

Director, Product Management
XYPRO Technology Corporation
HP NonStop Server Security
and Encryption Solutions