May 17, 2019

To
Dr. Lilly Chen,
Dr. Morris Dworkin,
NIST

Re. a proposal for NIST - “AES-GCM-SIV“

As NIST is no doubt aware, the GCM block-cipher mode specified in SP 800-38D causes significant concerns when used in a context where nonces cannot be trivially generated from a counter.

Currently, there are six pages of FIPS 140-2 implementation guidance concerning themselves with this problem and the safest answer - random generation - limits a key to 2^32 plaintexts.

Enclosed, we propose a solution, named “AES-GCM-SIV”, that addresses the problem of nonce reuse and also: a) enables larger numbers of messages to be encrypted per key, with improved security bounds; b) uses the same primitives as GCM, and thus is still able to benefit from the commonly available AES and binary-field instructions in current processors.

This mode is not as fast as AES-GCM because, by definition, the nonce misuse resistance property requires two passes over the data. As a result, encryption with AES-GCM-SIV is a bit slower than AES-GCM, although on modern platforms it is still possible to encrypt with AES-GCM-SIV at a cost of less than 1 cycle per byte. Fortunately, decryption is parallelizable and can be performed at the same rate as AES-GCM.

We believe that the improved security properties and extension of the lifetime of a key more than compensate for that, and commend it to you in contexts where GCM is questionable.

AES-GCM-SIV has been publicly reviewed by the CFRG/IETF for about three years, and has recently been published as RFC 8452: AES-GCM-SIV [1].

Other related available resources are:

- Reference and optimized code [2]
- Implementations integrated into the open source library BoringSSL [3]
- A detailed description and discussion of the security of AES-GCM-SIV [4]
- Nonce-Based Key Derivation [5]

Please consider our proposal, and do not hesitate to contact us if any additional information is required.

Thank you,
Shay Gueron, Adam Langley, Yehuda Lindell

References:

[1] S. Gueron, A. Langley and Y. Lindell, “AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption”, RFC 8452 (2019) https://tools.ietf.org/html/rfc8452
[2] https://github.com/Shay-Gueron/AES-GCM-SIV
[3] https://boringssl.googlesource.com/boringssl/
[4] S. Gueron, A. Langley and Y. Lindell, “AES-GCM-SIV: Specification and Analysis”, IACR ePrint http://eprint.iacr.org/2017/168.pdf

[5] S. Gueron, Y. Lindell, “Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation”, 24th ACM CCS conference (2017) https://dl.acm.org/citation.cfm?doid=3133956.3133992 [see also https://eprint.iacr.org/2017/702]