ERICSSON

Date: October 9, 2023

Ericsson AB
Group Function Technology
SE-164 80 Stockholm
SWEDEN

Comments on SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

Dear NIST,

Thanks for your continuous efforts to produce well-written open-access security documents.

Please find below additional comments on SP 800-38D:

- *"if n denotes the total number of blocks in the encoding (i.e., the input to the GHASH function in the definition of S in Secs. 7.1 and 7.2 above) of the ciphertext and AAD"*

  We suggest that this is changed to "if m denotes …". In 6.4, m denotes the total number of blocks in the encoding. In Section 6.5, n denotes the total number of blocks in the plaintext.

- Appendix B discusses the authentication assurance and explains that the forgery probability is $\approx n/2^t$ where n is the total number of blocks in the encoding of the ciphertext and AAD and t is the tag length. We think this information is very useful for the reader but gives a too negative image of GCM authentication assurance. We think the document should also explain that when t = 128, 96-bit IVs are used (which is the only length that should ever be used), and $\sigma + q + q' < 2^{64}$, the integrity advantage is $\lesssim q'(\ell_A + 1)/2^{127}$ where σ is the total number of blocks in all plaintexts, q is the number of encryption queries, q' is the number of decryption queries, and ℓ_A is the maximum input length in blocks. This follows from equation (22) and Section 7.5 in the paper "Breaking and Repairing GCM Security Proofs" by Iwata et al. [1]. An integrity advantage linear in q' is theoretically optimal and much better than the integrity advantage of CCM with 128-bit tags, which is quadratic in q [2] (but note that for small t, ℓ_A, q and q' CCM behaves as an ideal MAC with an integrity advantage of $\lesssim q'/2^t$). GCM's integrity advantage is also much better than the integrity advantage of OCB with 128-bit tags, which is quadratic in σ [3] and better than the integrity advantage of ChaCha20-Poly1305, which is $\lesssim q'(\ell_A + 1)/2^{103}$ [4]. As noted in [5], the integrity advantage of GCM can be written as $\lesssim (v + 1)(\ell_A + 1)/2^{127}$ where v is the number of forgery attempts (failed AEAD decryption invocations).

- Similar to Appendix B, we think SP 800-38D should also discuss the confidentiality assurance and explain that the confidentiality advantage of AES-GCM is only $\lesssim \sigma^2/2^{129}$ where σ is the total number of encrypted blocks. After sending 2^{20} messages of length 2^{20} blocks, the confidentiality advantage is only $\lesssim 1/2^{49}$. This is much worse than e.g., ChaCha20, AEGIS, and sponge functions such as Ascon

and Keccak in duplex mode. The GCM confidentiality advantage is questionably low, especially when used with AES-256. The Sweet32 attack [6] has sparked increased interest in distinguishing attacks and the subpar confidentiality advantage of AES-CTR leads to frequent re-keying in protocols such as TLS 1.3 that aims for high theoretical security margins.

– *"In particular, if IVs are ever repeated for the GCM authenticated encryption function for a given key, then it is likely that an adversary will be able to determine the hash subkey from the resulting ciphertexts."*

  We think it would be very good if this is explained in more detail, so that it is easy to understand that this attack is very easy to perform in practice. In a recent discussion in 3GPP people questioned if the attack is practical. Our understanding from [7] is that even with a single IV collision it is on average very practical for an attacker to brute force the possible values of H. With two collisions or more, the number of possible values is on average very small and finding H is trivial.

– SP 800-38D allows randomly-chosen IVs and states that *"The probability that the authenticated encryption function ever will be invoked with the same IV and the same key on two (or more) distinct sets of input data shall be no greater than* 2^{-32} *"* and *"The total number of invocations of the authenticated encryption function shall not exceed* 2^{32}*"*.

  If r random 96-bit IVs are used with the same key, the collision probability for AES-GCM is $\approx r^2/2^{97}$ where a collision breaks both confidentiality and integrity. As described in [8], as an attacker can test r IVs (or keystreams) for collisions with work r, by storing them in a hash table, the time complexity of such an attack is $2^{97}/r$, and the security of AES-GCM with random IVs is only $\approx 97 - \log_2 r$. This is much lower than the 128-bit security expected for AES-128 and the 256-bit security expected for AES-256. For $r = 2^{32}$, the security level is 65 bits.

  As an IVs collision has worse consequences than a successful forgery or a distinguishing attack and the security with just two random IVs ($r = 2$) is below the expected 128-bit security level expected by AES-128 and very far below the 256-bit security level expected by AES-256 we think NIST should discourage the use of AES-GCM with random IVs.

Best Regards,
John Preuß Mattsson,
Expert Cryptographic Algorithms and Security Protocols

[1] Iwata, Ohashi, Minematsu, “Breaking and Repairing GCM Security Proofs”
https://eprint.iacr.org/2012/438.pdf

[2] Jonsson, "On the Security of CTR + CBC-MAC"
https://doi.org/10.1007/3-540-36492-7_7

[3] Rogaway, Bellare, Black, “OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption”
https://www.cs.ucdavis.edu/~rogaway/papers/ocb-full.pdf

[4] Procter, "A Security Analysis of the Composition of ChaCha20 and Poly1305"
https://eprint.iacr.org/2014/613.pdf

[5] Günther, Thomson, Wood, “Usage Limits on AEAD Algorithms”
https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-limits/

[6] Bhargavan, Leurent, “Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN”
https://sweet32.info/

[7] Joux, “Authentication Failures in NIST version of GCM”
https://csrc.nist.gov/csrc/media/projects/block-cipher-techniques/documents/bcm/comments/800-38-series-drafts/gcm/joux_comments.pdf

[8] Preuß Mattsson, Smeets, Thormarker, “Proposals for Standardization of Encryption Schemes”
https://csrc.nist.gov/csrc/media/Events/2023/third-workshop-on-block-cipher-modes-of-operation/documents/accepted-papers/Proposals%20for%20Standardization%20of%20Encryption%20Schemes%20Final.pdf