Public Comments on the Decision Proposal to Convert FIPS 198-1 to a NIST Special Publication

Comment period: September 20, 2022 - October 20, 2022

On September 20, 2022, NIST's Crypto Publication Review Board announced a proposal to convert Federal Information Processing Standard (FIPS) 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*, to a NIST Special Publication.

The comments that NIST received on the proposal during the comment period (September 20, 2022 to October 20, 2022) are collected below.

More information about this review is available from NIST's Crypto Publication Review Project site.

LIST OF COMMENTS

1. Comments from Ryan Wagner, Google, October 20, 2022

Introduction

This document provides comments to the four changes proposed in the "Announcement of Proposal to Convert FIPS 198-1 to a NIST Special Publication" [1], namely:

1. Convert FIPS 198-1 to a NIST Special Publication (SP)
2. Update the HMAC specification to include block sizes for the SHA-3 family of hash functions
3. Include a discussion on truncation
4. Improve the editorial quality and update references

1. **Convert FIPS 198-1 to a NIST Special Publication (SP)**

Overall, this seems to be a good move since FIPS documents have historically been the venue for the publication of low-level cryptographic primitives standards (e.g. AES and SHA), while SP documents for the publication of constructions built on top of the former group.

It is not clear whether this change will somehow impact FIPS validation processes and would appreciate NIST clarification on this matter. .

2. **Update the HMAC specification to include block sizes for the SHA-3 family of hash functions**

HMAC has been created specifically to remediate length-extension attacks which affect Merkle-Damgard hash functions, such as SHA1 and SHA2 families, in the context of message authentication. In particular, it is insecure to use the following construction as a MAC:

Construction 1: MAC(K, M) = hash(K || M)

where "hash" is a Merkle-Damgard hash function, "K" stands for a cryptographic key, "M" for the message, and "||" for concatenation. This situation led to the development of the much more involved the Construction 2, which requires at least two calls to the underlying hash function:

Construction 2: HMAC(K, M) = H((K' \xor opad) || H((K' \xor ipad) || M),

where K' = H(K), if K is larger than the block size of H,
or K' = K (padded with zeros if needed), otherwise.

Length-extension vulnerability does not apply to SHA3 (it was one of the security requirements presented in Section III of the SHA-3 competition call for proposals [2]). For this reason, it is safe to use the more efficient **Construction 1** for SHA3, also known as KMAC, which is already defined in NIST SP 800-185 [2].

Given the above, standardizing a SHA3-based HMAC construction does not seem reasonable. It would still be a secure construction but the issue is that it will be rather inefficient when compared to the already standardized KMAC (at least two hash computations vs one).

Generalist software engineers might not have the above cryptographic expertise, and may end up picking an HMAC-SHA3 construction because it seems a smoother transition from an existing HMAC-SHA2 or HMAC-SHA1 deployment. This would lead to latency increase for these applications. In addition, miscommunication problems would exist given the existence of two NIST-endorsed MAC constructions based on SHA-3.

NIST and the cryptographic community need to make as much effort as possible to prevent these misunderstandings.

3. **Include a discussion on truncation**

This is a great change. The existing discussion about truncation in FIPS 198-1 is incipient, pointing to only a single paragraph in NIST SP 800-107. This is a topic of great relevance in practice since many applications cannot afford the usual MAC output length.

4. **Improve the editorial quality and update references**

No objections.

References

[1]: Announcement of Proposal to Convert FIPS 198-1, "The Keyed-Hash Message Authentication Code (HMAC)," to a NIST Special Publication. NIST, September 20, 2022. https://www.nist.gov/news-events/news/2022/09/announcement-proposal-convert-fips-198-1-keyed-hash-message-authentication

[2] Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family. NIST. 11/02/2007. https://www.federalregister.gov/documents/2007/11/02/E7-21581/announcing-request-for-candidate-algorithm-nominations-for-a-new-cryptographic-hash-algorithm-sha-3

[3] SP 800-185. SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash. https://csrc.nist.gov/publications/detail/sp/800-185/final