From: clinton bowen <clinton.bowen@gmail.com>
Sent: Thursday, August 14, 2014 10:32 AM
To: internal-hash
Subject: My Comments on DRAFT FIPS 202

1) The comment:

I'm addressing this for the cause of trouble in the future. For cryptography (i.e. not security, e.g. security -> FIPS 140 & 199), I recognize that FIPS documents that are purposed to define cryptographic primitives and SP documents related to cryptography build upon the cryptographic primitives defined in FIPS publications. All functions before SHA3 defined in FIPS publications are primitives. SHA3 isn't a primitive cryptographic function. SHA3 is a composition of a primitive cryptographic permutation function with a sponge (and a pad). FIPS has never seen a permutation function as a cryptographic primitive. FIPS 202 should emphasize approved permutations (e.g. Keccak-p[b, n_r]), approved sponges with corresponding padding function(s). The SHA3 definition should be an Annex of FIPS 202 because it is a specific instance of a sponge with corresponding pad and a cryptographic primitive Keccak-p[b, n_r].

The reason for all of this is to accommodate the possibility of future approved sponges and permutations. The SHA-3 standardization page has pdf's of what is planned after FIPS 202: authenticated encryption, PRF, tree hashing, RNG. Secondly the call for papers for the NIST Hash workshop at CRYPTO 2014 already implies that the duplex sponge will be approved in some instance in the future by NIST. Whether these modes belong in a FIPS or SP document is up to NIST. The way FIPS 202 is written now, I don't see how it leaves room for other planned uses of sponges and permutations. Decades from now we'll want to read verbiage from FIPS 202 like "…use this sponge with a FIPS 202 Annex A approved permutation function…" or "… SHA4 is defined as Sponge#2[Permutation#4, Pad#6, r]". This kind of verbiage is consistent with other FIPS and SP documentation. A fortiori, the Keccak team presented a concept of this in "Keccak and the SHA-3 Standardization" that is found on the SHA-3 standardization page (see page 50/60).

2) Proposal:

FIPS 202 could be compartmentalized like FIPS 140 is compartmentalized (I don't care if it is one document or several documents). Annexes below C (i.e. D, E, F, and G) should specify the composition and modes of uses of the permutations and sponges defined in Annex A and Annex B respectively. The outline of FIPS 202 could be conceptualized as follows:

a. FIPS 202 "Permutation-Based Cryptography":
    i. A high level description of sponges and cryptographic permutations
    ii. A disclaimer that cryptographic permutations are to be used with sponges. Something similar to section 7 of the current draft.
    iii. Some verbiage on how FIPS 202 is compartmentalized.
b. Annex A: Approved Permutation Functions
    i. Keccak-p[b, n_r] -> place section3 to 3.4 of the current draft in here.
    ii. Part 2 could be left for future approved permutations.
c. Annex B: Approved Sponge Functions
    i. Sponge[f,pad,r](M,d) -> place section 4 and 5.1 of the current draft in here.
    ii. reserve part 2 for Duplex[f,pad,r](sigma, L) should it be approved in the near future.
    iii. Part 3 could be left for future approved sponges. Examples of other types of sponges are the donkey sponge and the monkey duplex sponge
d. Annex C: Security Analysis of Permutation-Based Cryptography

i. Ask the keccak team and the academic cryptographic community nicely for help with Annex C.

e. Annex D: Approved Permutation-Based Hash and Extendable-Output Functions
   i. Fixed length hash functions:
      1. SHA3 -> Place section 5.2, 6, 6.1 of the current draft in here. My opinion is that 5.2, 6, and 6.1 could be merged.
   ii. Extendable Output functions:
      2. SHAKE -> Place section 6.2 of the current draft in here
   iii. Object Identifiers
      3. Don't be lazy. Place the actual identifiers of Appendix A.3 of the current draft in here. Remember, we're not going to have access to that page of the internet at all times, but perhaps we'll have a copy of the annex.

f. Annex E: Approved Permutation-Based Pseudo-random functions
   i. …

g. Annex F: Approved Permutation-Based Encryption & Authenticated Encryption Methods
   i. Encryption Methods:
      1. …
   ii. Authenticated Encryption Methods:
      1. …

h. Annex G: Approved Permutation-Based Stream Ciphers
   i. …

My opinion is that tree hashing and DRBG's using sha-3 or any other approved permutation based hash functions belong in SP documents and not Annexes of a FIPS since they are built around functions defined in Annex D.

3) Justification of proposal:

While this competition was supposed to result in a new hash function, the winner is really a new category(ies) of cryptographic functions, permutations with sponges. The resulting FIPS document should not be written as a document for a focused intent of hashing. It should be written for a new category of cryptography – a category that is quite flexible and can serve multiple purposes in cryptography and accommodate new uses of permutation based cryptography in the future.

Thanks,

--
-Clinton M. Bowen