From: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com>
Sent: Tuesday, August 26, 2014 6:33 PM
To: internal-hash
Subject: Comments on FIPS-202

In the FIPS 202 draft, you introduce a new cryptographical primitive called a XOF. Now, you list two things people may want to do with it:

- Generate a variable length hash
- Use it as a random-looking function (as in a KDF, or an OAEP masking function)

Now these are two separate scenarios; as a hash, we assume that the attacker picks the input (and we hope he can't control the output); as a KDF, he has only probabilistic information about the input (and we hope he can't use that to obtain probabilistic information about the output).

Now, a use of a XOF as a hash (at least, as you define SHAKE-128 and SHAKE-256) isn't very interesting; for XOF output length less than the security level, that hash obviously has a weaker security level, and so it's no better than taking (say) SHA3 output and truncating it. For XOR output length greater than the security level, you don't claim any extra security, and so (from a cryptographical perspective) it's no better than taking (again) SHA3 output and adding a bunch of 0 bits.

Now, using a XOF as a KDF is rather more interesting; however defining the security properties is a lot trickier. You state the hope that SHAKE128/SHAKE256 would defend against "attacks that would be resisted by a random function of the requested length…"; that certainly states what our intuition says we want (however, it's not clear how you'd be able to come up with a formal definition of that).

My suggestion is that you don't approve an XOF as a variable length hash (because it doesn't really bring anything to the table); instead you treat it strictly as a KDF (or something that needs similar security properties).

Also, you mention that the primitive might be a bit tricky to use (because of the prefix property); on the other hand, if the user dislikes the prefix capability, he can easily avoid it by including the output length as part of the data being hashed. You might want to make that suggestion in the (future) document that describes how XOF's are allowed to be used.

--
Scott Fluhrer