From: hash-forum@nist.gov on behalf of Kelsey, John M. <john.kelsey@nist.gov>
Sent: Friday, November 01, 2013 12:49 PM
To: HASH-FORUM
Subject: Moving forward with SHA3

Everyone,

We've been discussing what should go in the draft SHA3 FIPS among ourselves since the shutdown ended.

First, we are not going to try to move forward with the proposed version of SHA3 I presented at CHES. We were and are comfortable with that version on technical grounds, but the feedback we've gotten indicates that a lot of the crypto community is not comfortable with it.

This leaves us with the decision of what to put into the draft FIPS. All the feedback we've gotten by email and blog posts and phone calls and such is useful, and we definitely listen and take it into account, but the comments we *have* to address will come from the public comment period on the draft FIPS. Our hope is to get the draft FIPS out reasonably soon, then get public comments, address them, and eventually send it up to the Secretary of Commerce to sign. In order for that to happen, we want to put out a draft FIPS that is broadly acceptable to the community of cryptographers and crypto engineers and users of cryptography that will ultimately be using SHA3.

We considered two ways to move forward.

a. The new Keccak team proposal:

All fixed-length hashes have c=512, and thus a maximum of 256 bits of preimage resistance. Additionally, there are SHAKEs with c=256 and c=512.

b. The original fixed-length capacities plus the SHAKEs:

All n-bit fixed-length hashes have c = 2n, and thus offer 2^n preimage resistance. Additionally, there are SHAKEs with c=256 and c=512, allowing users of the variable-length hashes to choose a security level of either 128 or 256 bits.

Both of these options are technically defensible. On the side of the Keccak team's new proposal, neither NIST nor the rest of the crypto world spends much time on security against attacks that demand more than 2^{256} work. (We've come to agree with those who pointed out, during the SHA3 competition, that designing an algorithm with security beyond 2^{256} is pretty pointless.) On the side of the original capacities, it seems safest to have drop-in replacements that give identical or superior security guarantees to the SHA2 hashes they're intended to be able to replace, and that don't change what most people expect from fixed-length hash functions. Also, in the past, far more problems have been caused by demanding too much performance from hash functions than have been caused by demanding too much overdesign.

Our best understanding is that the performance difference between (a) and (b) will rarely matter--people looking for higher performance will generally use the 224- or 256-bit hashes (compatible with smaller and faster elliptic curve parameters).

Further, the process issues that have been brought up recently (basically, the feeling that it is improper or questionable to make big changes to the submitted SHA3 hashes) make an argument for putting out a draft FIPS with the original fixed-length capacities.

Finally, many people have objected to changing the security requirements for the SHA3 from those originally specified for SHA3 submissions.

Based on this reasoning, we are planning to go forward with a draft SHA3 FIPS with all the n-bit fixed hashes having capacity = 2n, thus providing n-bit preimage resistance. (That is the same preimage resistance that was originally required for submissions to the SHA3 competition.) The variable-length SHAKE functions will be defined (following Richie Frame's suggestion) in terms of a security level--either the 128-bit security level (c=256) or the 256-bit security level (c=512).

Fixed-length hashes:

SHA3-224 with c=448
SHA3-256 with c=512
SHA3-384 with c=768
SHA3-512 with c=1024

Variable-length hashes:

SHAKE128 with c=256
SHAKE256 with c=512

All these SHA3/SHAKE hashes will incorporate the Keccak team's Sakura padding.

Our plan is to get a draft FIPS out based on this plan relatively soon, and then to go out for public comments.

Comments?

--John