SHA-256 Today And Maybe Something Else in a Few Years: Effects on Research and Protocols

There is a widespread belief that SHA-256 will be the “hash function of choice” for use in security protocols unless it is replaced by a different function chosen by an international competition. In the AES competition, there was no well-accepted competitor before the competition began; for hashes, the existence and wide-scale deployment of SHA-256 changes the tenor of the competition significantly. The competition may feel like “how can we be better than SHA-256” instead of "how do we pick the best hash".

Another difference between block ciphers and hash functions will make the two competitions have very different properties. Before the AES competition, there was a general belief that the cryptographic community really understood block cipher design; today, there is a great deal of trepidation about whether or not the cryptographic community knows how to design a good hash function. Thus, the AES competition looked realistic from the outset, but for hash functions, it is quite unclear if a competition will lead to anything definitive.

Similarly, protocol developers and the standards bodies that drive them have gotten serious about updating protocols to allow different hash and signature algorithms to be used. In doing so, most are today naming SHA-256 as the successor to SHA-1 and MD5. This makes the transition to a different hash algorithm later both easier (because the protocols will be more agile) and more difficult (because users will be reluctant to make a second change without really strong proof of need).

This panel will consider how the existence of SHA-256 will affect the serious research that is needed to hold a meaningful hash competition, and how the outcome of the competition might be deployed in security protocols. Issues include:

- Encouraging cryptographic research into attacking SHA-256 with the goal being having better requirements for the competition

- Thinking about how having SHA-256 as a known competitor changes the type of research people will do for developing competitors

- Assessing whether or not the pervasiveness of SHA-256 will slant the process of deciding which features are important for the competition

- If, in the end, something other than SHA-256 is chosen, understanding what will be needed to get the protocols and their users to change to the chosen function

Proposed moderator: Arjen Lenstra

Possible panelists:

Hashes: Paulo Barreto, Niels Ferguson, John Kelsey. Antoine Joux, Bart Preneel, Vincent Rijmen, others who are working on weaknesses in SHA-256 and/or who have developed non-Merkle-Damgård hashes

Protocols: Paul Hoffman, Russ Housley, Eric Rescorla