From: hash-forum@nist.gov on behalf of Burr, William E. [william.burr@nist.gov]

Sent: Thursday, December 09, 2010 5:25 PM

To: Multiple recipients of list

Subject: The SHA-3 Finalists

NIST has selected five SHA-3 candidate algorithms to advance to the third (and final) round:

- BLAKE
- Grøstl
- JH
- Keccak
- Skein

The selection was challenging, because we had a strong field of fourteen hash algorithms remaining in the SHA-3 competition that were very strong contenders for the hash function standard. Security was our greatest concern, and we took this very seriously, but none of these candidates was clearly broken. However, it is meaningless to discuss the security of a hash function without relating security to performance, so in reality, NIST wanted highly secure algorithms that also performed well. We preferred to be conservative about security, and in some cases did not select algorithms with exceptional performance, largely because something about them made us "nervous," even though we knew of no clear attack against the full algorithm.

Performance is multidimensional: no algorithm excelled in every dimension. Every second-round candidate achieved at least tolerable performance on mainstream desktop or server systems, although the performance range was significant. There were bigger differences on constrained platforms and in hardware, where area is as much a performance factor as speed. A couple of algorithms were wounded or eliminated by very large area requirements – it seemed that the area they required precluded their use in too much of the potential application space. Some algorithms allowed very high levels of fine-grain parallelism that could be realized well with hardware, some exploited parallelism with vector units, and some seemed to fully exploit the considerable parallelism that can be achieved by conventional superscalar arithmetic logic units (ALUs) that can simultaneously launch several instructions per clock cycle. Several algorithms also exploited the power of 64-bit-wide ALUs.

No algorithm survived to become a finalist that did not have a clear round structure that could be readily adjusted to trade security for performance. NIST eliminated several algorithms because of the extent of their second-round tweaks or because of a relative lack of reported cryptanalysis – either tended to create the suspicion that the design might not yet be fully tested and mature. NIST was generally comfortable with tweaks to the number of rounds or to constants, but more suspicious of changes that seemed to affect the structure of the compression functions.

Some teams announced the tweaks that they would make if they were selected for the final round. NIST evaluated the second-round submissions, but not the proposed tweaks. However, we did consider whether the best attacks on some of the candidates seemed amenable to mitigation by a simple modification.

NIST also considered diversity in the selection of the finalists. The selected five finalists incorporated a number of new design ideas that have arisen in the last few years, such as the HAIFA and sponge hash constructions. The finalists include designs whose nonlinearity is based on the AES S-box, on a smaller (4- or 5-bit wide) S-box efficiently implemented as a sequence of basic logical instructions, and on the interaction between addition and XOR operations.

NIST thanks the submitters of all fourteen second-round candidates. Every second-round candidate was a very professional effort, and every candidate had strong features to recommend it. We also thank the many individuals and organizations who helped with the cryptanalysis of the candidates, or who provided performance data from their own implementations of the candidate algorithms. This selection would not have been possible without their help.

NIST will publish a report on the selection of the SHA-3 finalists in the near future that explains the rationale for the selections on an algorithm-by-algorithm basis.

If tweaks are being considered for the final round, the submissions are due on January 16, 2011. Specific submission requirements will be provided to the designers of the five SHA-3 finalists.

Bill Burr

William E. Burr
Manager, Cryptographic Technology Group
NIST
Phone: 301-975-2914
Fax: 301-975-8670