National Institute of Standards and Technology
Information Technology Laboratory

SEARCH CSRC: ⬚ GO

ABOUT   MISSION   CONTACT   STAFF   SITE MAP

CSRC HOME   GROUPS   PUBLICATIONS   DRIVERS   NEWS & EVENTS   ARCHIVE

Cryptographic Hash Project

Cryptographic Hash Algorithm Competition

Timeline for Hash Algorithm Competition

Federal Register Notices

NIST Policy on HASH Functions

NIST Comments on SHA-1 Cryptanalysis

First Cryptographic Hash Workshop

Second Cryptographic Hash Workshop

Email Mailing List

Contacts

Other Links

NIST COMMENTS ON CRYPTANALYTIC ATTACKS ON SHA-1

In 2005 Prof. Xiaoyun Wang announced a differential attack on the SHA-1 hash function; with her recent improvements, this attack is expected to find a hash collision (two messages with the same hash value) with an estimated work of 2^{63} operations, rather than the ideal 2^{80} operations that should be required for SHA-1 or any good 160-bit hash function. This is a very large computation, and to our knowledge nobody has yet verified Prof. Wong's method by finding a SHA-1 collision, but 2^{63} operations is plainly within the realm of feasibility for a high resource attacker. NIST accepts that Prof. Wang has indeed found a practical collision attack on SHA-1.

NIST held a workshop to consider the status of hash functions on Oct. 31-Nov. 1, 2005 and has reviewed the implications of Prof. Wang's attack. The attack primarily affects some digital signature applications, including timestamping and certificate signing operations, where one party prepares a message for the generation of a digital signature by a second party, and third parties then verify the signature. There are many applications of hash functions, and many do not require strong collision resistance; for example, keyed hash applications, such as the Hash-based Message Authentication Code (HMAC) or key derivation applications of hash functions do not seem to be affected.

Several steps are now prudent. The first of these is to transition rapidly to the stronger "SHA-2" family of hash functions (SHA-224, SHA-256, SHA-384 and SHA-512) for digital signature applications. The SHA-2 hash functions are in the same general family of hash functions as SHA-1. They could potentially be attacked with similar techniques, but they are much stronger than SHA-1. Practical SHA-2 attacks are unlikely in the next decade; and might never be found, except through decades of exponential growth of available computing power. The SHA-2 hash functions are well along in the commercial system deployment process and are available in many newer systems and applications, but are not yet available in the majority of deployed systems. The primary constraint on the current use of the SHA-2 hash functions for signatures is interoperability; many relying party systems do not yet implement them, and may not do so for several more years. NIST encourages a rapid adoption of the SHA-2 hash functions for digital signatures, and, in any event, Federal agencies must stop relying on digital signatures that are generated using SHA-1 by the end of 2010.

The second step is to encourage hash function research to better understand hash function design and attacks in preparation for selecting additional hash functions. The cryptographic community is in a period of rapid development in the theory of hash functions and their cryptanalysis. NIST plans to host additional hash function workshops; the next of these will be held on Aug. 24-25, 2006 in Santa Barbara, California to follow immediately after the Crypto 2006 Conference.

The third step will be a hash function competition, similar to the successful Advanced Encryption Standard (AES) development and selection process. The schedule for this competition has not yet been determined, but presupposes a sense of sufficient maturity and stability in hash function theory and technology, that the results will improve on or otherwise complement the SHA-2 hash functions, and will occur before the current hash functions are determined to be insecure. NIST does not have strong preconceptions about the number of new hash functions to be selected from this competition, since the very broad range of hash function applications may argue for two or more specialized hash functions.

William E. Burr

NIST
Manager, Security Technology Group
301-975-2914

October 17, 2007