X-Sieve: CMU Sieve 2.2
Date: Fri, 27 Apr 2007 16:58:53 +0900
From: Atsuhiro Yamagishi <a-yamagi@ipa.go.jp>
User-Agent: Thunderbird 1.5.0.10 (Windows/20070221)
To: hash-function@nist.gov, shu-jen.chang@nist.gov
CC: cryptrec-sec4@cryptrec.jp
Subject: Re: REMINDER - comment period on NIST's hash function requirements
 to end in 5 weeks on 4/27/07
X-Proofpoint-Virus-Version: vendor=fsecure engine=4.65.5502:2.3.11,1.2.37,4.0.164
definitions=2007-04-27_02:2007-04-26,2007-04-27,2007-04-27 signatures=0
X-PP-SpamDetails: rule=spampolicy2_notspam policy=spampolicy2 score=0 spamscore=0
ipscore=0 phishscore=0 adultscore=0 classifier=spam adjust=0 reason=mlx engine=3.1.0-
0703060001 definitions=main-0704270004
X-PP-SpamScore: 0
X-NIST-MailScanner: Found to be clean
X-NIST-MailScanner-From: a-yamagi@ipa.go.jp

Dear Dr. Shu-jen

We are glad to send the comments to "draft requirements and evaluation
criteria for new hash functions".
Those comments are the comments as CRYPTREC.
The comments from the member of CRYPTREC was collected in the CRYPTREC
secretariat.

Best Regards
Atsuhiro Yamagishi
Secretariat of CRYPTREC

Atsuhiro Yamagishi
Cryptography Research Group
IT Security Center(ISEC)
Information-technology Promotion Agency, JAPAN(IPA)
Bynkyo Green Court Center Office
2-28-8 Honkomagome, Bunkyo-ku
Tokyo, 113-6591 JAPAN
Phone : +81-3-5978-7508
Fax : +81-3-5978-7518

Public comments FROM CRYPTREC.pdf are below.

Public comments on the development of new hash algorithms for the revision of Federal Information Processing Standard (FIPS) 180-2, Secure Hash Standard

General comments

- It should be reminded again why NIST succeed in the AES competition. Well-studies on the security requirements for block ciphers seem to bring the success; however, it is not necessarily the case for hash functions. Thus a lack of studies on the hash function might make people discuss more the performance aspects than the security ones. NIST should revise the competition schedule and take more time to decide AHS.
- The security requirements for hash function depend on what it is used for. The present NIST requirements for AHS specification seem insufficient for not only security requirements but performance requirements. As for security requirements, it is desirable for AHS to be secure for 50 years at least because the replace of hash algorithm costs industries a lot.
- The size of message digest and the number of rounds are important for the security; however it should be also considered other criteria for it.

Detailed comments

A. Proposed Draft Minimum Acceptability Requirements for Candidate Algorithms

Comment on A. 1： During the competition, all the candidates are free of use if they are used for research activities. After the competition, only the winner must abort the patent.

Comment on A. 2：It should be refer to smart card platform.

B. Proposed Draft Submission Requirements

Comment on B. 1 ： The original NIST requirement describes that the documentation for new algorithm should suggest modification techniques; however it should not be allowed to tweak the algorithm arbitrary. It should be only allowed to select the parameters, for example, the number of round, output length and so

on.

Comment on B. 2 : It should be described what language and what platform the optimize code works on.

C. Proposed Draft Evaluation Criteria of Candidate Algorithms

Comment on C. 1 :

(1) The evaluation criterion "indistinguishability from a random oracle" may be misleading. A random oracle is an ideal black-box random function. Thus, indistinguishability from a random oracle may be regarded as pseudorandomness. In the definition of pseudorandomness, a hash function H should be treated as a function family $H_k(x) = H(k, x)$, where k is a part of the input of H and k is chosen uniformly at random and kept secret. However, a hash function is not fed any secret piece of input when used for the instantiation of a random oracle. It seems difficult to define formally the suitability of a hash function for instantiation of a random oracle. Some necessary conditions may be near-collision resistance, near-2^{nd}-preimage resistance and near-preimage resistance. For example, near-preimage resistance means that, for a given y, it is difficult to obtain x such that the Hamming distance between y and $H(x)$ is small.

(2) The future AHS is also expected to be used for constructing a MAC function such as HMAC in FIPS PUB 198 and a pseudorandom number generator such as Hash_DRBG in NIST SP800-90. Thus, it seems better to require explicitly a mode of a hash function as a function with secret input.

Comment on C. 3. 1 : The algorithm should be parameterizable, e.g. can accommodate additional rounds and arbitrary output length.

Remark: Each comment comes from different people having different backgrounds.