Blue Midnight Wish – update

Presentation prepared by

Svein Johan Knapskog[1] and Danilo Gligoroski[2]

1. Centre for Quantifiable Quality of Service in Communication Systems (Q2S) - Centre of Excellence
2. Department of Telematics

Faculty of Information Technology, Mathematics and Electrical Engineering

Norwegian University of Science and TechnologyTechnology - NTNU, NORWAY

Outline

- The BMW Team (recently enlarged)
- The Efficiency of a Hash Function
- Security Status of BMW
- NIST Hash Function Competition – Phase 3

The BLUE MIDNIGHT WISH Team (recently enlarged)

- Danilo Gligoroski (designer)
- Vlastimil Klima (designer)
- Svein Johan Knapskog (team coordinator, general comments and suggestions for improvements, proofreading)
- Mohamed E. E. H. Aly (VHDL, FPGA and ASIC implementations)
- Jørn Amundsen (Big-endian and endian-neutral implementation, suggestions for improvements and optimizations)
- Stig Frode Mjølsnes (initial contribution with 8-bit implementation)
- Rune Erlend Jensen (**new member**, specializing in x86 and x64 optimizations and keeping BMW on the top of the supercop charts)
- Daniel Otte (**new member**, specializing in optimizations for embedded 8-bit, 16-bit, 32-bit processors, keeping BMW on the top of comparative charts)

Preliminary Determination by the ITC

The ITC will preliminarily determine, within 25 days after the date on which it receives notice of the initiation, whether there is a reasonable indication that imports of subsidized LWTP from the PRC are causing material injury, or threatening to cause material injury, to a U.S. industry. *See* section 703(a)(2) of the Act. A negative ITC determination will result in the investigation being terminated; otherwise, the investigation will proceed according to statutory and regulatory time limits.

This notice is issued and published pursuant to section 777(i) of the Act.

Dated: October 29, 2007.

Stephen J. Claeys,

Acting Assistant Secretary for Import Administration.

[FR Doc. E7–21616 Filed 11–1–07; 8:45 am]

BILLING CODE 3510–DS–S

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 070911510–7512–01]

Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA–3) Family

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice and request for nominations for candidate hash algorithms.

SUMMARY: This notice solicits nominations from any interested party for candidate algorithms to be considered for SHA–3, and specifies how to submit a nomination package. It presents the nomination requirements and the minimum acceptability requirements of a "complete and proper" candidate algorithm submission. The evaluation criteria that will be used to appraise the candidate algorithms are also described.

DATES: Candidate algorithm nomination packages must be received by October 31, 2008. Further details are available in section 2.

ADDRESSES: Candidate algorithm submission packages should be sent to: Ms. Shu-jen Chang, Information Technology Laboratory, *Attention:* Hash Algorithm Submissions, 100 Bureau Drive—Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930.

FOR FURTHER INFORMATION CONTACT: For general information, send e-mail to *hash-function@nist.gov*. For questions related to a specific submission package, contact Ms. Shu-jen Chang, National Institute of Standards and Technology, 100 Bureau Drive—Stop 8930, Gaithersburg, MD 20899–8930; telephone: 301–975–2940 or via fax at 301–975–8670, e-mail: *shu-jen.chang@nist.gov*.

SUPPLEMENTARY INFORMATION: This notice contains the following sections:

Recently, cryptanalysts have found collisions on the MD4, MD5, and SHA–0 algorithms; moreover, a method for finding SHA–1 collisions with less than the expected amount of work has been published, although at this time SHA–1 collisions have not yet been demonstrated. Although there is no specific reason to believe that a practical attack on any of the SHA–2 family of hash functions is imminent, a successful collision attack on an algorithm in the SHA–2 family could have catastrophic effects for digital signatures.

NIST has decided that it is prudent to develop a new hash algorithm to augment and revise FIPS 180–2. The new hash algorithm will be referred to as "SHA–3" and will be developed

NIST expects SHA–3 to have a security strength that is at least as good as the hash algorithms currently specified in FIPS 180–2, and that this security strength will be achieved with significantly improved efficiency. NIST

fixed size message digests so that a digest could act as a proxy for a possibly very large variable length message in a digital signature algorithm, such as RSA or DSA. These hash functions have since been widely used for many other "ancillary" applications, including hash-based message authentication codes, pseudo random number generators, and key derivation functions.

A series of related hash functions have been developed, such as MD4, MD5, SHA–0, SHA–1 and the SHA–2 family, (which includes 224, 256, 384 and 512-bit variants); all of these follow the Merkle-Damgard construct. NIST began the standardization of the SHA hash functions in 1993, with a specification of SHA–0 in the Federal Information Processing Standards Publication (FIPS PUBS) 180, the Secure Hash Standard; subsequent revisions of the FIPS have replaced SHA–0 with SHA–1 and added the SHA–2 family in FIPS 180–1 and FIPS 180–2, respectively.

NIST's overall hash algorithm toolkit. Therefore, the submitted algorithms for SHA–3 must provide message digests of 224, 256, 384 and 512 bits to allow substitution for the SHA–2 family. The 160-bit hash value produced by SHA–1 is becoming too small to use for digital signatures, therefore, a 160-bit replacement hash algorithm is not contemplated.

Many cryptographic applications that are currently specified in FIPS and NIST Special Publications require the use of a NIST-approved hash algorithm. These publications include:

- FIPS 186–2, Digital Signature Standard;
- FIPS 198, The Keyed-Hash Message Authentication Code (HMAC);
- *SP* 800–56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography; and
- *SP* 800–90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (DRBGs).

The SHA–3 algorithm is expected to be suitable for these applications.

Since SHA–3 is expected to provide a simple substitute for the SHA–2 family of hash functions, certain properties of the SHA–2 hash functions must be preserved, including the input parameters; the output sizes; the collision resistance, preimage resistance, and second-preimage resistance properties; and the "one-pass" streaming mode of execution. However, it is also desirable that the selected SHA–3 algorithm offer features or properties that exceed, or improve upon, the SHA–2 hash functions. For example, the selected SHA–3 algorithm may offer efficient integral options, such as randomized hashing, that

ission package (and in the hash algorithm ocess), candidate ssion packages must wing (as described in

pecifications and mentation. ia. Property Statements/ closures. mission Requirements. ms is discussed in

shall contain the ation: submitted algorithm. bmitter's name, e-mail ne, fax, organization, ss.

application.

For interoperability, NIST strongly desires a single hash algorithm family (that is, that different size message digests be internally generated in as similar a manner as possible) to be selected for SHA–3. However, if more than one suitable candidate family is identified, and each provides significant advantages, NIST may consider recommending more than one family for inclusion in the revised Secure Hash Standard.

2. Requirements for Candidate Algorithm Submission Packages

Candidate algorithm nomination packages must be received by October 31, 2008. Submission packages received before August 31, 2008 will be reviewed for completeness by NIST; the submitters will be notified of any deficiencies by September 30, 2008, allowing time for deficient packages to be amended by the submission deadline. No amendments to packages will be permitted after the submission deadline. Requests for the withdrawal of submission packages will only be honored until the submission deadline.

Due to the specific requirements of the submission package such as Intellectual Property Statements / Agreements / Disclosures as specified in section 2.D, e-mail submissions will not be accepted for these statements or for the initial submission package. However, e-mail submissions of amendments to the initial submission package will be allowed prior to the submission deadline.

"Complete and proper" submission packages received in response to this notice will be posted at *http://www.nist.gov/hash-competition* for inspection. To be considered as a

- Name(s) of auxiliary submitter(s).
- Name of the algorithm inventor(s)/ developer(s).
- Name of the owner, if any, of the algorithm. (normally expected to be the same as the submitter).
- Signature of the submitter.
- (optional) Backup point of contact (with telephone, fax, postal address, e-mail address).

2.B Algorithm Specifications and Supporting Documentation

2.B.1 A complete written specification of the algorithm shall be included, consisting of all necessary mathematical operations, equations, tables, diagrams, and parameters that are needed to implement the algorithm. The document shall include design rationale (e.g., the rationale for choosing the specific number of rounds for computing the hashes) and an explanation for all the important design decisions that are made. It should also include 1) any security argument that is applicable, such as a security reduction proof, and 2) a preliminary analysis, such as possible attack scenarios for collision-finding, first-preimage-finding, second-preimage-finding, length-extension attack, multicollision attack, or any cryptographic attacks that have been considered and their results.

In addition, the submitted algorithm may include a tunable security parameter, such as the number of rounds, which would allow the selection of a range of possible security/performance tradeoffs. If such a parameter is provided, the submission document must specify a recommended value for each digest size specified in Section 3, with justification. The submission should also provide any bounds that the designer feels are appropriate for the parameter, including a bound below which the submitter expects cryptanalysis to become practical. The tunable parameter may be used to produce weakened versions of the submitted algorithm for analysis, and permit NIST to select a different security/performance tradeoff than originally specified by the submitter, in light of discovered attacks or other analysis, and in light of the alternative algorithms that are available. NIST will consult with the submitter of the algorithm if it plans to select that algorithm for SHA–3, but with a different parameter value than originally specified by the submitter. Submissions that do not include such a parameter should include a weakened version of the submitted algorithm for analysis, if at all possible.

NIST is open to, and encourages, submissions of hash functions that differ from the traditional Merkle-Damgard model, using other structures, chaining modes, and possibly additional inputs. However, if a submitted algorithm cannot be used directly in current applications of hash functions as specified in FIPS or NIST Special Publications, the submitted algorithm must define a compatibility construct with the same input and output parameters as the SHA hash functions such that it can replace the existing SHA functions in current applications without any loss of security. The replacement of all SHA functions in any standardized application by this compatibility construct shall require no additional modification of the standard application beyond the alteration of any algorithm specific parameters already present in the standard, such as algorithm name and message block length. Submissions may optionally define other variants, constructs, or iterated structures for specific useful applications.

NIST worldwide hash competition for SHA-3

- What does “significantly improved efficiency” (over SHA-2) mean?
- Let us assume the following “definition”: Significantly improved efficiency over SHA-2 means **at least 2 times faster than SHA-2**.
- Then, if a function is 2 times slower than SHA-2, it means that it has significantly worse efficiency.
- This convention seems to be accepted by many in cryptography (see “Classification of the SHA-3 Candidates”, Fleischmann, Forler, and Gorski, eprint 2008, report 511)

Efficiency of the 14 SHA-3 candidates

32-bit Mode, 2400MHz, Intel Core 2 Duo,
Cycles/byte, eBASH, supercop-20100726, cobra

significantly more efficient than SHA-2
SHA-2
slower than SHA-2
significantly worse than SHA-2

	32-bit mode, 256 bit hash	Speed cycles/byte
1	Blue Midnight Wish	7.42
2		
3		
4		
5		
6		
7	SHA-256	15.42
8		
9		
10		
11		
12		
13		
14		
15		

	32-bit mode, 512 bit hash	Speed cycles/byte
1	Blue Midnight Wish	4.75
2		
3		
4		
5		
6	SHA-512	18.27
7		
8		
9		
10		
11		
12		
13		
14		
15		

NTNU
Innovation and Creativity

Efficiency of the 14 SHA-3 candidates

64-bit Mode, 2400MHz, Intel Core 2 Duo,
Cycles/byte, eBASH, supercop-20100726, cobra

significantly more efficient than SHA-2
SHA-2
slower than SHA-2
significantly worse than SHA-2

	64-bit mode, 256 bit hash	Speed cycles/byte
1	Blue Midnight Wish	5.95
2		
3		
4		
5		
6		
7		
8		
9	SHA-256	15.33
10		
11		
12		
13		
14		
15		

	64-bit mode, 512 bit hash	Speed cycles/byte
1	Blue Midnight Wish	3.59
2		
3		
4		
5	SHA-512	10.25
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		

Only one SHA-3 candidate significantly outperforms SHA-2 in all modes, for all 32 and 64 bits CPU architectures, for all digest sizes and for both short and long messages.

SHA-2

slower than SHA-2

significantly worse than SHA-2

	64-bit mode, 256 bit hash	Speed cycles/byte
1	**Blue Midnight Wish**	5.95
2		
3		
4		
5		
6		
7		
8		
9	SHA-256	15.33
10		
11		
12		
13		
14		
15		

	64-bit mode, 512 bit hash	Speed cycles/byte
1	**Blue Midnight Wish**	3.59
2		
3		
4		
5	SHA-512	10.25
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		

NTNU
Innovation and Creativity

Only one SHA-3 candidate significantly outperforms SHA-2 in all modes, for all 32 and 64 bits CPU architectures, for all digest sizes and for both short and long messages. Every other candidate manifest sometimes worse performances than SHA-2, in some mode, or for some digest size, or for some message length or for some processor architecture.

1	Blue Midnight Wish	5.95
2		
3		
4		
5		
6		
7		
8		
9	SHA-256	15.33
10		
11		
12		
13		
14		
15		

1	Blue Midnight Wish	3.59
2		
3		
4		
5	SHA-512	10.25
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		

NTNU
Innovation and Creativity

Cryptanalytic status of Blue Midnight Wish

- Not a single attack on the full hash function.
- No serious attack on the compression function.
- Several pseudo-distinguishers (or “banana attacks”) where attacker **controls everything** in the compression function of BMW will just increase the confidence in the hash function for the following reasons:
  1. They confirm the designers’ prediction that numerous entangled bijections and high diffusion present in BMW design will force attackers to fall into the trap of (or slip on) “banana” attacks.
  2. Any present and future pseudo-distinguisher attack is an explicit admittance that the attack is not affecting the security of the hash function because:
     - there is no freedom in choosing IV, and
     - there is no freedom in the last finalization call of the compression function.
- Consequently, we encourage more “banana attacks”

NIST Hash Function Competition - Phase 3, 2010 - 2012

- Security analyses will continue (Gligoroski, Klima, Ødegård, ...)
- Development and optimization
  - Software (Amundsen, Jensen, Otte, ...)
  - Hardware (El-Hadedy Aly, ...)
  - Embedded systems (Otte, cooperative efforts, ...)
- Demonstrators for relevant usage scenarios
- Further prototyping and measurements

Q2S

Thank you for your attention!

NTNU
Innovation and Creativity