X-Sieve: CMU Sieve 2.2
Subject: Hash Algorithm Requirements and Evaluation Criteria.
Date: Tue, 24 Apr 2007 15:33:18 -0400
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Topic: Hash Algorithm Requirements and Evaluation Criteria.
Thread-Index: AceGp2lMk80tV1PHRK6wNxCLGp10iQ==
From: "Ferrer, Daniel F." <ferre1df@cmich.edu>
To: <hash-function@nist.gov>
Cc: "Willoughby, Eric J" <willo1ej@cmich.edu>,
"Tang, Chunxia " <tang1c@cmich.edu>
X-OriginalArrivalTime: 24 Apr 2007 19:33:20.0315 (UTC) FILETIME=[6A3950B0:01C786A7]
X-CanItPRO-Stream: default
X-Spam-Score: undef - Message too big
X-Scanned-By: CanIt (www . roaringpenguin . com) on 141.209.20.21
X-Proofpoint-Virus-Version: vendor=fsecure engine=4.65.5502:2.3.11,1.2.37,4.0.164
definitions=2007-04-24_08:2007-04-23,2007-04-24,2007-04-24 signatures=0
X-PP-SpamDetails: rule=spampolicy2_notspam policy=spampolicy2 score=0 classifier= adjust=0
reason=limit engine=3.1.0-0703060001 definitions=main-0704240101
X-PP-SpamScore: 0
X-NIST-MailScanner: Found to be clean
X-NIST-MailScanner-From: ferre1df@cmich.edu

Tuesday, April 24, 2007

Regard: Hash Algorithm Requirements and Evaluation Criteria

TO:
Mr. William Burr, Attn: Hash
Algorithm Requirements and Evaluation
Criteria, National Institute of Standards
and Technology, 100 Bureau Drive, Stop 8930,
Gaithersburg, MD 20899–8930.

From:
Daniel Ferrer (and co-authors)
Library Systems Department
Park Library
Central Michigan University
Mount Pleasant, MI
48859
U.S.A.

Phone: 1-989-774-2338
E-mail: Daniel.Ferrer@cmich.edu

As you have requested comments:

[Docket No.: 061213336–6336–01]
Announcing the Development of New Hash Algorithm(s) for the Revision of
Federal Information Processing Standard (FIPS) 180–2, Secure Hash
Standard. “Federal Register” / Vol. 72, No. 14 / Tuesday, January 23, 2007 / Notices 2861

“The purpose of this notice is to solicit comments on the draft minimum
acceptability requirements, submission requirements, and evaluation criteria of

candidate algorithms from the public, the cryptographic community, academic/research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations so that their needs can be considered in the process of developing the augmented and revised hash function standard."

Please see attached documents.

"NIST's hash function competition: security and implementation issues"
By Daniel Fidel Ferrer(1), Eric Willoughby(1), and Chuxia Tang(2)
1 Central Michigan University Libraries
E-mail contact: Daniel.Ferrer@cmich.edu
2 Central Michigan University Research Corporation

One paper in three formats.
.pdf
.ps
.ps.gz

If you have any questions, please
contact Daniel Fidel Ferrer.

Thank you – Daniel Fidel Ferrer.

Daniel Fidel Ferrer (and co-authors)
Library Systems Department
Park Library
Central Michigan University
Mount Pleasant, MI
48859
U.S.A.

Phone: 1-989-774-2338
E-mail: Daniel.Ferrer@cmich.edu

End of message.

NISTHashpaper.pdf is below

TO:
Mr. William Burr, Attn: Hash
Algorithm Requirements and Evaluation Criteria
National Institute of Standards and Technology
100 Bureau Drive,
Stop 8930,
Gaithersburg, MD 20899–8930

DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
[Docket No.: 061213336–6336–01]
Announcing the Development of New Hash Algorithm(s) for the Revision of
Federal Information Processing Standard (FIPS) 180–2, Secure Hash Standard.

Request for comments:

"*NIST's hash function competition: security and implementation issues*"

By Daniel Fidel Ferrer[1], Eric Willoughby[1], and Chuxia Tang[2]

[1] Central Michigan University Libraries
E-mail contact: Daniel.Ferrer@cmich.edu
[2] Central Michigan University Research Corporation

Due to recent attacks (1) on the SHA-1 hash function on January 23, 2007, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) announced the instigation of an effort to develop new cryptographic hash algorithm(s) for the revision of Federal Information Processing Standard (FIPS) 180-2, the Secure Hash Standard (2). This general public program follows the similar earlier effort in January 1997, when NIST announced the initiation of the Advanced Encryption Standard (AES). The original AES development effort had made a formal call for algorithms on September, 1997 at which time fifteen AES candidate algorithms were selected (four were broken by 1999); and then October 2000 the Rijndael was the chosen as the finalist. By November 2001 the FIPS-197 Advanced Encryption Standard (AES) was published. Four years later, in 2005 a completely successful timing attack against AES was already published by Daniel J. Bernstein (3). A much earlier paper "A timing attack against Rijndael" by Francois Koeune and Jean-Jacques Quisquater was published as a technical report in June of 1999 (4), before Rijndael was selected. Interestingly enough it was Twofish that was said to be open to timing and power analysis attacks during the development of the AES. One paper suggested that AES would need to be good for encrypting for twenty years and secure or another twenty years (5). Perhaps it is already past time for NIST to initiate the Super Advanced Encryption Standard (SAES) competition along with the Secure Hash Standard. Conceivably, it should be called the Advanced Secure Hash Standard (ASHS) to be followed by the Super Advanced Secure Hash Standard (SASHS). From a historical point of view, there has indeed been cause for a loss of confidence in finding long-term encryption standards. The lengthy history of broken cryptographic standards is now a normal part of the study of

cryptology. In fact, currently American National Standards Institute (ANSI) X9 and International Organization for Standardization (ISO) with the International Electrotechnical Commission (IEC) SC27 have directed a five year review of published standards.

At this time, NIST has developed a timetable and a similar public selection process that was used for the Advanced Encryption Standard (AES) for the new Secure Hash Standard with a schedule of six years to select the award winner of the new hash function(s) and publish the new standard (6).

To begin with, there are the questions about the current proposed evaluation criteria: security, computational efficiency, memory requirements, hardware and software suitability, simplicity, flexibility, and licensing requirements. The weighting of each of these criteria is important and clearly the actual judgment and ranking of the candidates is of the utmost significance. The definitive analysis and ranking of the candidates leads to the final product that may be used for years to come in cryptographic systems. It is important to remember one of the best records so far was that of MD2, which survived 10 years of attacks.

Background security and implementation issues:

General problems abound with the implementation of AES. In the recent case of the timing attack against AES, Daniel J. Bernstein wrote, "Did NIST decide, after evaluating timing attacks, that those attacks were unimportant? No. Exactly the opposite occurred, as discussed below. So what went wrong? Answer: NIST failed to recognize that table lookups do not take constant time. "Table lookup: not vulnerable to timing attacks" NIST stated in [19, Section 3.6.2]. **NIST's statement was, and is, incorrect.**"(7). This was not a failure of the evaluation criteria or in understanding the type of attack; but rather, a complete failure in understanding the implementation security import. In other words, it is possible that the incorrect judgment was most likely done by a committee, but not reviewed by a competent implementation programmer. In the end, it was a devastatingly fatal flaw in how AES is currently implemented and the past evaluation process missed this completely.

In the recent *Federal Register* announcement, it is stated that "several of the non-NIST approved hash functions have been successfully attacked" (8); but the status of these recent attacks and other well known attacks against AES, for instance, are not mentioned. More importantly, the format used in the public competition that developed AES is seriously flawed and therefore needs to be completely re-thought. This paper is directed toward the task of re-thinking this process. The general open process (Shannon's maxim) that NIST used for AES is a good first step but the rest of the process and failures have to be examined systematically. Historical concerns over the standardization process with DES have not gone away, even though many people currently believe that the NSA worked to strengthen DES.

Most discussions of cryptographic protocols start out by discussing the quantitative and probabilistic issues strictly based on mathematical complexity. Increasingly, the theoretical theorem-proof paradigm of cryptology is of limited significance to real world cryptosystems, which if broken have extremely serious consequences. Statements like "it will take until the next ice age occurs before a computer the size of California will be able to calculate all of the possibilities to crack the encrypted text" are common. This leads one to think that cryptographic

security is solely a matter of mathematical certainty or elegant algorithms and has nothing to do with the way that encryption works in the real world of hardware, firmware, software, the networks, and actual program source code. The first myth is that the security, encryption protocols, and cryptosystems are a branch of mathematics that is **only** concerned with mathematical risks and soundness, computational difficulty, and probabilistic statistics. They suggest that applied cryptography is simply a matter of creating rigorously good algorithms. With this assumption, if cipher text could withstand brute-force attacks, then it is cryptographically secure. However, these simple ideas have been shown to be obsolete, since the entire protocol and cryptosystem have to be implemented securely as well. Is cryptography a branch of mathematics or a case of applied computer science? Real world cryptosystems are applied computer science.

To make a simple point, a Secure Hash Standard is not actually done and processed in an ideal world on paper (or a formal model); but rather, it specifically goes through a complex series of hardware, firmware, software, memory, human programmer's source code at different levels, diverse operating systems, wireless nodes, and thousands of miles through space and across worldwide optical fiber and wire networks, Indeed, cryptosystems increasingly need to be able to operate successfully in mobile battery-powered systems, which are more susceptible to power monitoring attacks or differential power analysis (DPA). In other words, encryption standards operate in a complex world-wide physical and virtual environment. Assurances can only given by degree.

What does it mean for a cryptographic protocol and standard to be "secure"? How do cryptosystems fail and how are they broken? There are clearly mathematical proofs (soundness) that give a rigorous mathematical solution of some level of security; however, there are many other types of attacks that have shown that there are significant weaknesses in some awfully good and sound cryptographic protocols. Why do some cryptographic protocols even "feel weak" to cryptologists? Many of the successful attacks have happened at the edges (perimeters, cryptographic boundary) not at the center and the strongest part of the algorithm. What would it mean to have secureful science that would render cryptanalysis as a science and not as a "black art" done in "black chambers"? The concept of cryptographic strength is a contradiction in terms. The level of certainty needed equates to the risk of a successful attack being almost zero. The securement from all known attacks would be the primary goal. Although the security can be thought of as the lack or absence of risk, in fact, there are only degrees of security. Remember during the development of the standards, attempts to break the candidates are a good thing; computer hackers are on our side. The so called Black Hat security meetings are a case in point for computer and cryptographic hackers developing ways of attacking cryptosystems. Another example would be Sandia IORTA's Red Teams that hunt for security holes and do vulnerability analysis to guard against cyber-terrorist attacks.

In the past exceedingly good encryption was previously only important in the military (again we have Americans in harm's way) and the intelligence or diplomatic realm; but now in the Internet business/eBay world and our information society in general, it has become essential for maintaining privacy and security in the new billion dollar and growing online economy. Although the recent *Federal Register* announcement said, "capable of protecting sensitive government information well into the foreseeable future" (9), and indeed, the PUBLIC LAW

107–347—DEC. 17 2002 is generally aimed at governmental systems, it is clear that the larger information business systems and the worldwide Internet community have a huge stake in the cryptographic standards like the Secure Hash Standard. In addition, the Public Law mentioned "To reduce costs and burdens for businesses" (10) as a goal. The price of a cryptographic failure could be enormous in today's market place. The cost of the standardization process for the Secure Hash Standard is less than that of the selection in the American Idol TV program (Fox); however, the Secure Hash Standard's security will have a more profound effect on the public's trust worldwide. In the past, other national and transnational standards organizations have reviewed and systematically evaluated American cryptographic standards. Two such examples are, the New European Schemes for Signatures, Integrity, and Encryption (NESSIE) and Japan's Cryptography Research and Evaluation Committee (CRYPTREC).

The standard and process needs to directly address the implementation issues to some degree in order for the concrete implementation (ANSI C source language reference implementation) on different computers in the real world. This helps the whole and entire encryption process to be strong and secure against all known attacks. Real world attack-testing and cryptanalysis of the total process needs to be done, not just functional and compliance testing or a simple brute force attack. Functional testing will never truly reveal a secure system; interoperability requirements are only important for actual secure systems. Even one time pads can be broken – remember the "VENONA" project started in 1946 is a historical example of implementation errors being successfully exploited (11). It is now said that the decryption rate of the Soviet NKVD cables was 49% in 1944 (12).

The question as to the role of the National Security Agency/Central Security Service (NSA/CSS) in the entire process needs to be defined and addressed. In the past, the SHA-0 development to SHA-1 (1995) was done by input from the NSA, who also helped get SHA-1 at least to this point. Thus, it is clear that the NSA input should be included in the formal process. The NSA has designed and constructed encryption devices at least for the military, so we may assume that they have been involved in real world attack-testing. At one time, there was a separate group at the NSA called Engineering, Technology and Research (ETR); the research likely has included attack testing. This is an obvious area for the NSA to work on cryptanalysis of the candidates, but one serious caveat needs to be stated before this process starts. There must be a way for the NSA to communicate real failures by candidate algorithms without divulging any governmental secrets (if they were used) as to how the candidates were broken. This sticky concern needs to be addressed before the evaluation process starts. Given the fact that the NSA employs the nation's premier cryptologists they need to be included in the formal and the official process of reviewing the candidates. In reference to the NSA, remember what President Truman (October 24, 1952, 55 years ago) said when he first established the NSA; his memorandum says "ensure the mobilization and the effective employment of the best available human and scientific resources in the field of cryptologic research and development." (13).

The relationship between the NIST and the NSA specifically with regard to the standards process is in fact mentioned in Public Law 107-347 Dec 17, 2002 (116 STAT. 2958), where it says, "**SEC. 303. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.** DEVELOPMENT OF STANDARDS AND GUIDELINES…consult with other agencies and offices and the private sector (including the Director of the Office of Management and Budget,

the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, and the Secretary of Homeland Security." Even though this part of the cryptologist's team may need to follow the motto of their greatest that "They Served in Silence", it is important to use our best resources on this task standardization. An example of such a group might be the NSA's National Information Assurance Research Laboratory (NIARL), which interacts with corporations in the private sector.

During the AES evaluation the NIST called on the NSA to work on "Initial Plans for Estimating the Hardware Performance of AES Submissions" (14). Their final report was given as "Hardware Performance Simulations of Round 2 Advanced Encryption Standard Algorithms" (15). This report was about "hardware performance". There were three individuals who worked for the NSA that were the co-authors. This is an important consideration, but in the future these studies would be better done by the microchip industry, who would know where the industry is headed in the next five to ten years during the time the standard would actually be in use (see later recommendations).

Thus, the general recommendation is that the NSA and the nation's premier cryptologists would be used to "break" the candidates. This would cause protocol/standards developers to do some testing before submitting their proposals. Also, remember how we got from SHA-0 to SHA-1 was by the **de facto** use of the NSA working on breaking SHA-0. Therefore, the NSA should be officially (**de jure**) used to work on breaking candidates and the cryptanalysis of the candidates for the new Secure Hash Standard. In short, it is time to take the gloves off and face the possibility that all of the candidates may get broken. Security trusted must be earned through this evaluation process for the new Secure Hash Standard.

Recommendation for a structured public expert teams approach:

Public committees and conferences should not be ruled out as being unessential, but the selection criteria and the analysis of the factors for each candidate should be done by teams weighting each of the criteria or factors. Teams of three or five expert members should be selected to judge and rank each of the factors; however some additional crucial factors need to be included (see below). The structured process that the U.S. Department of Commerce, National Science Foundation, and the National Institute of Health have used in the past to review general grant requests should be used as a model to select these teams. When necessary the grant review process has also dealt with concerns of businesses that have proprietary information, governmental secrets, non-disclosure agreements, copyright, lawsuits, intellectual property, and patents, etc. Only the final end product needs to be free and unpatented ("royalty-free worldwide"). However, it is imperative that the evaluation process includes the whole "tool kit" (private, public, and governmental).

Obviously one the most important requirements for choosing each team would be that its respective members are "experts" in their fields and are willing to be involved in the multi-year process of selecting a new standard. The teams would develop their own public checklist for evaluation and rankings. Each of the teams could ask for public input on general or specific topics related to their criteria or factor that they were evaluating. This would be a more open and thus a better approach than having the NIST establish internal technical review teams (as was used in the AES evaluation process). Public forums would still be used, but only after intensive

analysis and research by the teams. This would provide a deeper understanding of the candidates and therefore would make failure less likely. Web pages, wikis, blogs, and RSS feeds could all be used by teams as part of the public evaluation process.

In the end, the NIST will still be in charge of the process, but with a different structure to get through the evaluation rounds. This may take more time to setup initially, but will yield a more secure final result. There is still a need to combine both formal and informal methodologies in reviewing, evaluating, and attacking the candidates.

Therefore, it is strongly recommended that the structured teams of public experts be the approach used for the new Secure Hash Standard evaluation process.

The current evaluation criteria or factors: security, computational efficiency, memory requirements, hardware and software suitability, simplicity, flexibility, and licensing requirements need to be re-examined. Clearly the security factor needs to be more than just mathematical soundness or formal theoretical attacks; the critical issue is the inclusion of real world attack testing.

Three additional evaluation recommendations:

One additional recommendation is the creation of a team (factor, criteria) selected from industry, which would include software/security firms and chip makers (for example, Intel, IBM, Advanced Micro Devices Inc, and Sun Microsystems) as well. In the recent *Federal Register* announcement, it seems that the memory requirements deal only with hardware suitability (16). Hardware evaluation needs to be more than a simple look at memory requirements and gate counts. The idea of building more encryption standards directly into the hardware (embedded) is now an important consideration for overall security. Even induced faults like glitch attacks and physical leakage have to be considered with hardware implementations (17). As a general rule embedded-hardware encryption provides a much higher level of security and assurance than simple software encryption solutions if engineered and tested correctly. Indeed, a "Hardware Implementation of Hash Function SHA-512" by Hongqiang Li and Changyun Miao has recently been reported in the literature (18). A team selected from the larger corporations makes sense. Part of the team would be from private security companies and large software companies (for example, Microsoft, IBM, Oracle, Apple). Another example, Microsoft may be able to extract a formal model from the ANSI C source code for the standard (19).

Therefore, it is strongly recommended that a criteria and a team be selected from industry and be included in the new Secure Hash Standard evaluation process.

A second recommendation which needs to be weighted profoundly is a team and a factor of "implementation security" (not just memory or speed). This team requires software engineers who are also cryptography experts. The issues of real world robust implementation are not secondary. A computational efficiency factor is of no importance for a failed (cracked, wounded, broken, defeatable) Secure Hash Standard. There are many catastrophic flaws in actual implementation of encryption software; indeed, many software security companies are making money finding them. This shows that designing a sound and a perfect Secure Hash Standard and then waiting for the implementation issues to somehow become more secure over time is not

feasible. The implementation has to be considered as a real world engineering problem during the evaluation process and not just in principal, but in actual attack testing. Flaw remediation needs to happen immediately.

The general notion of a side channel attack where the implementation of the cryptosystem is insecure has to be addressed by implementation and engineering testing. For example, in 2003 Stefan Mangard published a Simple Power-Analysis (SPA) attack on an implementation of AES on smart cards (20). Ciphers need to be designed from the beginning with the assumption that leaked information derived from side-channel information may make them entirely vulnerable. Other cryptographic attacks have to be considered as well. Work on any serious cryptanalytic attacks will take time during the evaluation phases. For example, there is now a small industry of side-channel attacks (see the 17 papers listed at the "AES Lounge") (21) against the Advanced Encryption Standard (AES). Appropriate pragmatic implementation countermeasures and attack scenarios need to be addressed during the standards process, not as an after-thought or something minimized because of limited resources. Vulnerability analysis has to be at the forefront of the evaluation process, as we have seen what happens with failure and broken standards.

Therefore, it is strongly recommended that a criterion (factor) and a team for implementation security be included in the new Secure Hash Standard evaluation process.

The final recommendation is that a team and a factor of "networking" should be included in the requirements and be an essential part of the evaluation process. This is relevant since perhaps the largest application of the Secure Hash Standard might be used in a network environment (the Internet, etc) and networks have special security considerations. The United States government and The PUBLIC LAW 107–347—DEC. 17 2002 points directly to the matter of network applications. If the Secure Hash Standard candidate does not work extremely well in a network environment, then it is undoubtedly out of the competition. "The use of cryptography within networking applications often requires special considerations." (NIST, 19.3.5 Applying Cryptography to Networks) (22). Cryptosystems are specialized in a network environment, thus the networking issues cannot only be a diminutive part of the evaluation process. The data structure and protocols of Internet transactions are well known and have a long history of being fixed standards. In addition, it is possible to replace or modify the data in the traffic package and obtain results from these changes made by the attackers. End-to-end encryption and total link encryption is an important part of the implementation of a cryptographic standard in a public network.

There are on-going discussions about network encryption with regards to IPsec, IPv6, the matter of Encapsulated Security Payload (ESP), bit-flipping (ESPv2), and the wide-ranging Internet2 project. These will all have a direct impact on networking in the next ten years. In addition, it has been reported that IPv6 is the foundation of interoperability for the DoD's Global Information Grid (GIG). The Office of Management and Budget (OMB) has mandated that US Government agencies incorporate IPv6 capability into parts of their networks by 2008 in preparation for an eventual implementation. Thus, network encryption is undergoing radical design changes in the next few years and is an extremely important part of the worldwide need for secure standards.

Therefore, it is strongly recommended that "networking" should be a separate factor and criteria for the new Secure Hash Standard evaluation process.

Conclusion:

The goal is for the new Secure Hash Standard to last longer than the six years it takes to do the standardization process!

References:

Note: the views and conclusions of this paper are those of the authors and do not represent the official polices of any organization. This paper was done under the auspices of the NIST call "to solicit comments on the draft minimum acceptability requirements, submission requirements, and evaluation criteria of candidate algorithms from the public" (*Federal Register,* 1/23/2007).

1). "NIST Comments on Cryptanalytic Attacks on SHA-1". Accessed 4/16/2007. http://www.csrc.nist.gov/pki/HashWorkshop/NIST%20Statement/Burr_Apr2006.html

2). Hash Algorithm(s) for the Revision of Federal Information Processing Standard (FIPS) 180–2, Secure Hash Standard. *Federal Register* / Vol. 72, No. 14 / Tuesday, January 23, 2007 / Notices 2861-2863. Docket No.: 061213336–6336–01]. Dated: January 16, 2007. James E. Hill.

3). "Cache-timing attacks on AES". By Daniel J. Bernstein. Accessed 4/16/2007. http://cr.yp.to/antiforgery/cachetiming-20050414.pdf

4). "A timing attack against Rijndae". By Francois Koeune and Jean-Jacques Quisquater, technical report CG-1999/1, Universite catholique de Louvain, UCL Crypto Group Technical Report Series. http://citeseer.ist.psu.edu/cachedpage/282820/1 Accessed 4/16/2007.

5). "Cryptanalytic Progress: Lessons for AES". By John Kelsey Niels Ferguson, Bruce Schneier, and Mike Stay. 30-Sep-2002. From the web page: "Public Comments on AES Candidate Algorithms - Round 2". http://csrc.nist.gov/CryptoToolkit/aes/round2/comments/20000501-jkelsey-1.pdf Accessed: 4/16/2007.

6). "Tentative Timeline of the Development of New Hash Functions". http://www.csrc.nist.gov/pki/HashWorkshop/timeline.html Accessed: 4/16/2007.

7). "Cache-timing attacks on AES". By Daniel J. Bernstein. Accessed 4/16/2007. http://cr.yp.to/antiforgery/cachetiming-20050414.pdf

8). *Federal Register* / Vol. 72, No. 14 / Tuesday, January 23, 2007 / Notices, page 2862.

9). *Federal Register* / Vol. 72, No. 14 / Tuesday, January 23, 2007 / Notices, page 2861.

10). PUBLIC LAW 107–347—DEC. 17 2002 116 STAT. p. 2901 number 6.

11). http://www.nsa.gov/venona/ Accessed: 4/16/2007.

12). http://en.wikipedia.org/wiki/VENONA_project Accessed: 4/16/2007.

13). President Truman's Memorandum for the Secretary of State, the Secretary of Defense. Subject: Communications Intelligence Activities. October 24, 1942. A20707 5/4/54/OSO. Harry S. Truman. http://www.nsa.gov/truman/truma00001.pdf Accessed: 4/16/2007. Page 8.

14). "Initial Plans for Estimating the Hardware Performance of AES Submissions". By National Security Agency. http://csrc.nist.gov/CryptoToolkit/aes/round2/nsahardware-aes.pdf Accessed: 4/16/2007.

15)." Hardware Performance Simulations of Round 2 Advanced Encryption Standard Algorithms". By Bryan Weeks, Mark Bean, Tom Rozylowicz, and Chris Ficke (National Security Agency). http://csrc.nist.gov/CryptoToolkit/aes/round2/NSA-AESfinalreport.pdf Accessed: 4/16/2007.

16). *Federal Register* / Vol. 72, No. 14 / Tuesday, January 23, 2007 / Notices, page 2863.

17). "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols". By Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, and Niraj K. Jha. IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 5, NO. 2, FEBRUARY 2006. Page(s): 128-143.

18). "Hardware Implementation of Hash Function SHA-512". By Hong-qiang Li; Chang-yun Miao; Innovative Computing, Information and Control, 2006. ICICIC '06. First International Conference._Volume 2, 30-01 Aug. 2006. Page(s): 38-42. Digital Object Identifier 10.1109/ICICIC.2006.289.

See also:
"Efficient single-chip implementation of SHA-384 and SHA-512". By McLoone, M. McCanny. This paper appears in: Field-Programmable Technology, 2002. (FPT). Proceedings. 2002 IEEE International Conference on Publication Date: 16-18 Dec. 2002. Page(s): 311-314. INSPEC Accession Number: 7726090.

19). "Provable Implementations of Security Protocols". By Andrew D. Gordon. Proceedings of the 21st Annual IEEE Symposium on Logic in Computer Science (LICS'06). 12-15 Aug. 2006 Page(s): 345-346

20). "A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion". By Stefan Mangard in P.J. Lee and C.H. Lim (Eds.): ICISC 2002, LNCS 2587. Page(s): 343-358. 2003.

21). “AES Lounge” web page. http://www.iaik.tugraz.at/research/krypto/AES/ Accessed: 4/16/2007. Subheadings: AES & Side-Channel Analysis and AES & Fault Analysis
After reading the articles, the question is how secure is AES now? The AES process and the strength of the winner have to be called in to question. No matter how elegant the algorithm was thought to be at the time.

22). “An Introduction to Computer Security: The NIST Handbook”.
Special Publication 800-12. By National Institute of Standards and Technology Technology Administration U.S. Department of Commerce.
http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf Accessed: 4/16/2007.

Tuesday, April 24, 2007.

Contact:

E-mail contact: Daniel.Ferrer@cmich.edu

Daniel Fidel Ferrer
Library Systems Department
Park Library
Central Michigan University
Mount Pleasant, Michigan 48859
U.S.A.

End.