DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Notice of Jointly Owned Inventions Available for Licensing

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice of jointly owned inventions available for licensing.

SUMMARY: The inventions listed below are jointly owned by the U.S. Government, as represented by the Department of Commerce. The inventions are available for licensing in accordance with 35 U.S.C. 207 and 37 CFR part 404 to achieve expeditious commercialization of results of federally funded research and development.

FOR FURTHER INFORMATION CONTACT: Technical and licensing information on these inventions may be obtained by writing to: National Institute of Standards and Technology, Office of Technology Partnerships, Attn: Mary Clague, Building 820, Room 213, Gaithersburg, MD 20899. Information is also available via telephone: (301) 975–4188 , fax (301) 869–2751, or e-mail: *mary.clague@nist.gov.* Any request for information should include the NIST Docket number and title for the invention as indicated below.

SUPPLEMENTARY INFORMATION: NIST may enter into a Cooperative Research and Development Agreement (''CRADA'') with the licensee to perform further research on the invention for purposes of commercialization. The inventions available for licensing are:

[NIST DOCKET NUMBER: 02–004US]

Title: Bio-Affinity Porous Matrix in Microfluidic Channels.

Abstract: This invention is jointly owned by the U.S. Government, as represented by the Department of Commerce, and Loyola College. Acrylamide-modified DNA probes are immobilized in polycarbonate microfluidic channels via photopolymerization in a polyacrylamide matrix. The resulting polymeric, hydrogel plugs are porous under electrophoretic conditions and hybridize with fluorescently-tagged complementary DNA. The double stranded DNA can be chemically denatured and the chip may be reused with a new analytical sample. Conditions for photopolymerization, hybridization, and denaturation are discussed. The photopolymerization of plugs containing different DNA probe sequences in one microfluidic channel, thereby enabling the selective detection of multiple DNA target in one electrophoretic pathway are demonstrated.

[NIST DOCKET NUMBER: 05–003US]

Title: Macro/Micro Crane.

Abstract: This invention is jointly owned by the U.S. Government, as represented by the Department of Commerce, and Oceaneering International, Inc. The invention describes a crane concept to facilitate the transfer of containerized cargo between two ships at sea. The invention uses a macro/micro design under which a serial set of independently controlled manipulators move a load between a base ship and a target ship. The manipulator is a modified container crane mounted on a ship subject to the actions of sea and wind. The modification compensates for the large motions of the base ship. The micro-manipulator moves the load and compensates for the motions of the receiving ship and the unscheduled motions of the base ship remaining after the macro-manipulator compensation.

Dated: June 7, 2005.

Hratch G. Semerjian,

Acting Director.

[FR Doc. 05–11730 Filed 6–13–05; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcing a Public Workshop on Cryptographic Hash

AGENCY: National Institute of Standards and Technology (NIST).

ACTION: Notice of public workshop.

SUMMARY: A vulnerability was recently identified in the NIST-approved cryptographic hash algorithm, *Secure Hash Algorithm-1* (SHA–1). In response, NIST is announcing a public workshop to discuss this vulnerability, assess the status of other NIST-approved hash algorithms, and discuss possible near- and long-term options.

DATES: The workshop will be held on October 31 and November 1, 2005, from 9 a.m. to 5:30 p.m.

ADDRESSES: The workshop will be held in the Green Auditorium, Building 101 at the National Institute of Standards and Technology, Gaithersburg, MD. Comments, presentations, and papers, including reports on preliminary work, are encouraged prior to the workshop and should be sent to: *hash-function@nist.gov.* A detailed draft agenda and supporting documentation for the workshop will be available prior to the workshop at: *http://www.nist.gov/hash-function.* The Web address for workshop registration is: *http://www.nist.gov/conferences/.*

FOR FURTHER INFORMATION CONTACT: Additional information, when available, may be obtained from the Cryptographic Hash Workshop Web site or by contacting Sara Caswell, NIST, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930. (301) 975–4634; Fax (301) 948–1233, or e-mail *sara@nist.gov.* Questions regarding workshop registration should be addressed to Teresa Vicente on (301) 975–3883 or *teresa.vicente@nist.gov.*

SUPPLEMENTARY INFORMATION: A cryptographic hash function takes a variable length input string and generates a fixed length output called the message digest. Because the message digest can serve as a digital fingerprint on the input, a cryptographic hash function is an important primitive in various security applications, such as authentication, key derivation, and digital signatures. One of the most commonly used hash functions is the NIST-approved SHA–1; however, a vulnerability has recently been uncovered that affects SHA–1. Specifically, a team of researchers reported that the SHA–1 function offered significantly less collision resistance than could be expected from a cryptographic hash function of its output size. Since all NIST-approved cryptographic hash functions share basic design attributes, a SHA–1 vulnerability warrants a reassessment of the entire family of the NIST-approved Secure Hash Algorithms. The Cryptographic Hash Workshop aims to solicit public input on how to respond to the current state of research in this area. Topics of specific interests include, but are not limited to, the following:

Security Status of Approved Hash Functions

- The latest results on the security of SHA–1;
- The latest results on the security of SHA–256 and SHA–512;
- Likely extensions to the latest results on the approved hash functions;
- The impacts of the latest results on different applications of the approved hash functions.

Short Term Actions

- How urgent are the current concerns with the approved hash functions?
- What changes to applications and protocols could mitigate potential problems?

- What guidance should NIST give with respect to hash functions and their applications?

Conditions for an Early Transition

- How can hash functions be assessed for security properties such as collision resistance, preimage resistance, and pseudo-randomness?
- What conditions would warrant a transition away from one of the approved hash functions earlier than currently planned?

Potential Replacement Options

- Hash functions currently available for replacing one of the approved hash functions;
- What paradigms, other than the Merkle-Damgård construction, might be appropriate to consider?
- The need for an open competition, along the lines of the AES competition, for designing a new hash function.

Requirements for Unkeyed Cryptographic Hash Functions

- Desirable (or undesirable) general properties of hash functions for security, performance, and implementability;
- Desirable (or undesirable) properties of hash functions for particular applications, such as digital signatures, key derivation, message authentication, and random number generation;
- Identifying and encouraging the proper use of hash functions for particular applications.

Submissions for the workshop are requested by July 15, 2005. NIST will provide the accepted papers and presentations in a workshop handout, and post them on the workshop Web site after the workshop. However, no formal workshop proceedings will be published. NIST encourages presentations and reports on preliminary work that participants plan to publish elsewhere.

Because of NIST security regulations, advance registration is mandatory; there will be no on-site, same-day registration. To register, please register via the Web at *http://www.nist.gov/conferences* or fax the registration form with your name, address, telephone, fax and e-mail address to (301) 948–2067 (Attn: Cryptographic Hash Workshop) by October 21, 2005. The registration fee will be $125.00 ($50.00 for students). Payment can be made by credit card, check, purchase order, or government training form. Registration questions should be addressed to Teresa Vicente on (301) 975–3883 or *teresa.vicente@nist.gov.*

Authority: This work is being initiated pursuant to NIST's responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Pub. L. 107–347.

Dated: June 7, 2005.

Hratch G. Semerjian,

Acting Director.

[FR Doc. 05–11729 Filed 6–13–05; 8:45 am]

BILLING CODE 3510–CN–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 060805A]

Fisheries off West Coast States and in the Western Pacific; Bottomfish Fisheries; Overfishing Determination on Bottomfish Multi-Species Stock Complex; Hawaiian Archipelago

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of overfishing determination.

SUMMARY: This action serves as a notice that NMFS, on behalf of the Secretary of Commerce (Secretary), has determined that overfishing is occurring on the bottomfish multi-species stock complex (bottomfish complex) around the Hawaiian Archipelago and requests the Western Pacific Fishery Management Council (Council) to take appropriate action to end this overfishing. The Council is required to take action to end overfishing within 1 year following notification by NMFS that overfishing is occurring. The intent of this notice is to inform interested persons that Hawaii's bottomfish complex is undergoing overfishing.

SUPPLEMENTARY INFORMATION: On May 27, 2005, NMFS sent the following letter to the Council that (1) notifies the Council of the determination that overfishing is occurring in the bottomfish complex around Hawaii, (2) explains the Council's obligation to act in response to a determination that overfishing is occurring, and (3) requests the Council to take appropriate action to end overfishing.

Mr. Roy Morioka, Chairman

Western Pacific Fishery Management Council

1164 Bishop Street, Suite 1400

Honolulu, HI 96813

Dear Roy,

By this letter, I advise the Western Pacific Fishery Management Council (Council) that NOAA's National Marine Fisheries Service (NMFS), on behalf of the Secretary of Commerce (Secretary), has determined that overfishing is occurring on the bottomfish multispecies stock complex (Complex) around the Hawaiian Archipelago, and to request the Council to take action to end that overfishing.

The Magnuson-Stevens Fishery Conservation and Management Act (Magnuson-Stevens Act) requires the Secretary to report annually on the status of fisheries within each regional fishery management council's geographical area of authority and identify those fisheries that are overfished or approaching a condition of being overfished (16 U.S.C. 1854(e)(1)). According to the guidelines for National Standard 1 of the Magnuson-Stevens Act (50 CFR 600.310), fishery stock status is assessed with respect to two status determination criteria, one of which is used to determine whether a stock is ''overfished'' and the second of which is used to determine whether the stock is subject to ''overfishing.'' A stock is considered to be overfished if its biomass falls below the minimum stock size threshold (MSST). A stock is subject to overfishing if the fishing mortality rate exceeds the maximum fishing mortality threshold (MFMT) for one year. The MSST and MFMT for particular stocks are specified in fishery management plans.

According to Amendment 6 Supplement to the Fishery Management Plan for the Bottomfish and Seamount Groundfish Fisheries of the Western Pacific Region (FMP), effective July 3, 2003 (68 FR 46112, August 5, 2003), the MFMT for bottomfish stock complexes managed under the FMP would be exceeded if the fishing mortality rate exceeded the rate associated with maximum sustainable yield (MSY). The most recent assessment of the Complex presented in Appendix 5 of the Bottomfish and Seamount Groundfish Fisheries of the Western Pacific Region 2003 Annual Report indicated that, based on data through 2002, fishing effort (proxy for fishing mortality) exceeded the rate associated with MSY.

Based on these assessment results, NMFS, relying on the expertise and advice of its Pacific Islands Fisheries Science Center, has determined that overfishing of the Complex is occurring around the Hawaiian Archipelago.

Appendix 5 points out that the main Hawaiian islands (MHI) is where the overfishing problem primarily occurs - ≥The MHI is the zone that contributes most of the problems in terms of both reduced biomass and overfishing.≥ Therefore, it is likely that reducing fishing mortality here would be the most effective means to end overfishing in the Hawaiian Archipelago.

We look forward to working together with the Council to develop a plan to end overfishing of bottomfish.

Sincerely,

William L. Robinson

Regional Administrator

Appendix 5 of the Council's 2003 Annual Report on the Bottomfish and Seamount Groundfish Fisheries of the Western Pacific Region is available from *http://www.wpcouncil.org/bottomfish.htm* (See: Preliminary 2003 Annual Report, Status of Bottomfish Stocks).