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?