

The Galois/Counter Mode of Operation (GCM) Cover Sheet for NIST Modes Submission

Principal submitter

David A. McGrew
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95032
(408) 525-8651
mcgrew@cisco.com

Auxiliary submitter

John Viega
Secure Software
4100 Lafayette Center Drive, Suite 100
Chantilly, VA 20151
(703) 814-4402
viega@securesoftware.com

The Galois/Counter Mode of Operation (GCM) was developed by the submitters in order to provide a provably secure and efficient high-speed authenticated encryption method that is free of intellectual property restrictions. This cover sheet outlines the submission of that mode for consideration in the National Institute of Standards and Technology's Modes of Operation process.

The main document contains the mode's specification, a summary of its properties, test vectors for the Advanced Encryption Standard, and performance estimates for both hardware and software. It also outlines efficient designs, illustrates the use of the mode for network encryption, and provides a rationale. Test vectors are also provided in separate files, which are contained in the compressed tar file `gcm-test-vectors.tar.gz`. The intellectual property statements is made in a separate document.