The Galois/Counter Mode of Operation (GCM) Intellectual Property Statement

David A. McGrew
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95032
mcgrew@cisco.com

John Viega
Secure Software
4100 Lafayette Center Drive, Suite 100
Chantilly, VA 20151
viega@securesoftware.com

The authors are unaware of any intellectual property rights that pertain to the Galois/Counter Mode of operation (GCM) [1], nor do they claim any such rights. The avoidance of such encumbrances was a specific design goal of the mode. It is based on methods that appeared in the literature over two decades ago: counter mode [3] and universal hashing [2].

References

[1] D. McGrew and J. Viega. The Galois/Counter Mode of Operation (GCM), *Submission to NIST Modes of Operation Process*, January 2004.

[2] M. Wegman and L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265279, 1981.

[3] W. Diffie and M. Hellman. Privacy and Authentication: An Introduction to Cryptography. *Proceedings of the IEEE*, Volume 67, Number 3, March, 1979.