Crypto Project 1

AES-GCM (AES in the Galois/Counter Mode)

Introduction:
http://en.wikipedia.org/wiki/Galois/Counter_Mode
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Primary specifications:
GCM: http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
GCM: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf
AES: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Available VHDL codes:
Codes of basic AES operations: aes_components.zip **(attached)**

Optimization Target:
Maximum Throughput/Area Ratio

Software implementations:
http://cryptojedi.org/crypto/#aesbs
http://www.cryptopp.com

Latest software performance numbers:
S. Gueron, "AES-GCM software performance on the current high end CPUs as a performance baseline for CAESAR competition," Proc. DIAC 2013, 11–13 August 2013, Chicago, USA, available at http://2013.diac.cr.yp.to/slides/gueron.pdf
E. Kasper and P. Schwabe, "Faster and Timing-Attack Resistant AES-GCM", CHES 2009 Lausanne, Sep. 2009, available at
paper: http://eprint.iacr.org/2009/129
slides:
http://www.chesworkshop.org/ches2009/presentations/01_Session_1/CHES2009_ekasper.pdf

Other resources:
http://ece.gmu.edu/coursewebpages/ECE/ECE545/F13/projects/crypto/1_GCM/GCM_resources.zip

Articles included in this zip file have the following reference information:

[1] B. Yang, S. Mishra and R. Karri, "High Speed Architecture for Galois/Counter Mode of Operation (GCM)," Cryptology ePrint Archive: Report 2005/146, 2005. http://eprint.iacr.org/2005/146.pdf

[2] D. McGrew and J. Viega, "The Galois/Counter Mode of Operation (GCM). Updated submission to NIST, Modes of Operation Process," 2005. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf

[3] J. Huo, G. Shou, Y. Hu, and Z. Guo, "The design and FPGA implementation of GF(2^128) multiplier for GHASH," Proc. International Conference on Network Security,

Wireless Communications and Trusted Computing, NSWCTC'09, Apr. 2009, pp. 554–557.

[4] L. Henzen and W. Fichtner, “FPGA parallel-pipelined AES-GCM core for 100G Ethernet applications,” Proc. European Solid State Circuits Conference, ESSCIRC 2010, Sep. 2010, pp. 202–205.

[5] G. Zhou, H. Michalik, “Efficient and High-Throughput Implementations of AES-GCM on FPGAs,” Proc. International Conference on Field-Programmable Technology 2007, ICFPT'07, Dec. 2007, pp. 185-192.

[6] J. Wang, G. Shou, Y. Hu, and Z. Guo, “High-speed architectures for GHASH based on efficient bit-parallel multipliers,” Proc. IEEE International Conference on Wireless Communications, Networking and Information Security, WCNIS'10, Jun. 2010, pp. 582–586.

[7] Y. Lu, G. Shou, Y. Hu, and Z. Guo, “The research and efficient FPGA implementation of Ghash core for GMAC,” Proc. International Conference on E-Business and Information System Security, EBISS'09, May 2009, pp. 1–5.

[8] A. Satoh, T. Sugawara, T. Aoki, "High-Performance Hardware Architectures for Galois Counter Mode," IEEE Transactions on Computers, vol. 58, issue 7, July 2009, pp. 917-930.

[9] P. Patel, "Parallel Multiplier Designs for the Galois/Counter Mode of Operation," MS Thesis, University of Waterloo, 2008.
http://libdspace.uwaterloo.ca/bitstream/10012/3789/1/Final%20Thesis%20%20Pujan%20Patel.pdf