# Cryptology ePrint Archive: Report 2011/385

### Efficient Implementation of Grand Cru with TI C6x+ Processor

*Azhar Ali Khan and Ghulam Murtaza*

**Abstract:** Grand Cru, a candidate cipher algorithm of NESSIE project, is based on the strategy of multiple layered security and derived from AES-128. This algorithm was not selected for second phase evaluation of NESSIE project due to implementation and processing cost. In this paper we present relatively a fast implementation of the cipher using Texas Instrument’s DSP C64x+.

**Category / Keywords:** implementation / Grand Cru, Keyed Structure of AES-128, DSP Implementation of

**Date:** received 15 Jul 2011

**Contact author:** azarmurtaza at hotmail com

**Available formats:** PDF | BibTeX Citation

**Version:** 20110715:113105 (All versions of this report)

**Discussion forum:** Show discussion | Start new discussion

[ Cryptology ePrint archive ]