Cryptology ePrint Archive: Report 2013/118

Throughput Optimized Implementations of QUAD

Jason R. Hamlet and Robert W. Brocato

Abstract: We present several software and hardware implementations of QUAD, a recently introduced stream cipher designed to be provably secure and practical to implement. The software implementations target both a personal computer and an ARM microprocessor. The hardware implementations target field programmable gate arrays. The purpose of our work was to first find the baseline performance of QUAD implementations, then to optimize our implementations for throughput. Our software implementations perform comparably to prior work. Our hardware implementations are the first known implementations to use random coefficients, in agreement with QUAD's security argument, and achieve much higher throughput than prior implementations.

Category / Keywords: QUAD, stream cipher, throughput optimization, hardware acceleration

Date: received 27 Feb 2013, last revised 13 May 2013

Contact author: jrhamle at sandia gov, rwbroca@sandia gov

Available formats: PDF | BibTeX Citation

Version: 20130513:162853 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]