Cryptology ePrint Archive: Report 2013/059

Optimized GPU Implementation and Performance Analysis of HC Series of Stream Ciphers

Ayesha Khalid and Deblin Bagchi and Goutam Paul and Anupam Chattopadhyay

Abstract: The ease of programming offered by the CUDA programming model attracted a lot of programmers to try the platform for acceleration of many non-graphics applications. Cryptography, being no exception, also found its share of exploration efforts, especially block ciphers. In this contribution we present a detailed walk-through of effective mapping of HC-128 and HC-256 stream ciphers on GPUs. Due to inherent inter-S-Box dependencies, intra-S-Box dependencies and a high number of memory accesses per keystream word generation, parallelization of HC series of stream ciphers remains challenging. For the first time, we present various optimization strategies for HC-128 and HC-256 speedup in tune with CUDA device architecture. The peak performance achieved with a single data-stream for HC-128 and HC-256 is 0.95 Gbps and 0.41 Gbps respectively. Although these throughput figures do not beat the CPU performance (10.9 Gbps for HC-128 and 7.5 Gbps for HC-256), our multiple parallel data-stream implementation is benchmarked to reach approximately 31 Gbps for HC-128 and 14 Gbps for HC-256 (with 32768 parallel data-streams). To the best of our knowledge, this is the first reported effort of mapping HC-Series of stream ciphers on GPUs.

Category / Keywords: secret-key cryptography / CUDA, eSTREAM, GPU, HC-128, HC-256, stream cipher

Publication Info: Accepted in 15th International Conference on Information Security and Cryptology (ICISC), November 28-30, 2012, Seoul, Korea.

Date: received 5 Feb 2013

Contact author: goutam paul at ieee org