Ulu, Metin Evrim; **Cenk, Murat**

A parallel GPU implementation of SWIFFTX. (English) Zbl 07441070

Slamanig, Daniel (ed.) et al., Mathematical aspects of computer and information sciences. 8th international conference, MACIS 2019, Gebze, Turkey, November 13–15, 2019. Revised selected papers. Cham: Springer. Lect. Notes Comput. Sci. 11989, 202-217 (2020)

Summary: The SWIFFTX algorithm is one of the candidates of SHA-3 Hash Competition that uses the number theoretic transform (NTT). It has 256-byte input blocks and 65-byte output blocks. In this paper, a parallel implementation of the algorithm and particular techniques to make it faster on GPU are proposed. We target version 6.1 of NVIDIA®CUDA™compute architecture that employs an ISA (Instruction Set Architecture) called Parallel Thread Execution (PTX) which possesses special instrinsics, hence we modify the reference implementation for better results. Experimental results indicate almost 10x improvement in speed and 5 W decrease in power consumption per 2^{16} hashes.

For the entire collection see [Zbl 1483.68012].

MSC:

68-XX Computer science
65-XX Numerical analysis

Keywords:

hash function; SWIFFTX; SHA-3; NTT; GPU; CUDA

Software:

CUDA; SWIFFT; CryptoStreams; EACirc; SWIFFTX

Full Text: DOI

References:

[1] Volkov, V.: Better performance at lower occupancy. Proc. GPU Technol. Conf

[2] Peikert, C., Rosen, A.: Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In: Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, 4-7 March 2006, Proceedings, pp. 145-166 (2006) · Zbl 1112.94020

[3] CUDA NVIDIA: NVIDIA CUDA C programming guide. Nvidia Corporation 120(18), 8 (2011)

[4] NVIDIA: Visual Profiler. https://docs.nvidia.com/cuda/profiler-users-guide/index.html. Accessed Apr 2018

[5] NVIDIA: Pascal Tuning Guide. https://docs.nvidia.com/cuda/pascal-tuning-guide/index.html. Accessed Apr 2018

[6] NVIDIA: Parallel Thread Execution ISA. https://docs.nvidia.com/cuda/parallel-thread-execution/index.html. Accessed Apr 2018

[7] NVIDIA: GeForce GTX 1080 Whitepaper. https://international.download.nvidia.com/geforce-com/international/pdfs/GeForce. Accessed Dec 2018

[8] Lyubashevsky, V., Micciancio, D., Peikert, C., Rosen, A.: SWIFFT: a modest proposal for FFT hashing. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 54-72. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-71039-4_4 · Zbl 1154.68403 · doi:10.1007/978-3-540-71039-4$_4$

[9] Lyubashevsky, V., Micciancio, D.: Generalized compact knapsacks are collision resistant. In: 33rd International Colloquium Automata, Languages and Programming, ICALP 2006, Venice, Italy, 10-14 July 2006, Proceedings, Part II, pp. 144-155 (2006) · Zbl 1133.68353

[10] Györfi, T., Cret, O., Hanrot, G., Brisebarre, N.: High-throughput hardware architecture for the swifft/swifftx hash functions. IACR Cryptology ePrint Archive, 2012:343 (2012)

[11] Centre for Research on Cryptography and Brno Czech Republic Security, Masaryk University. Tool for generation of data from cryptoprimitives (block and stream ciphers, hash functions). https://github.com/crocs-muni/CryptoStreams. Accessed Dec 2018

[12] Durstenfeld, R.: Algorithm 235: random permutation. Commun. ACM 7(7), 420 (1964)· doi:10.1145/364520.364540

[13] Arbitman, Y., Dogon, G., Lyubashevsky, V., Micciancio, D., Peikert, C., Rosen, A.: SWIFFTX: a proposal for the SHA-3 standard. In: The First SHA-3 Candidate Conference (2008)