Short Review on “A high-performance and energy-efficient exhaustive key search approach via GPU on DES-like cryptosystems”

Authors: Omid Hajihassani, Armin Ahmadzadeh, Saeid Gorgin [1]

Abstract

Recently, graphical processing units (GPUs) have found a prominent role in general-purpose applications. Specifically, in parallel processing applications where a considerable number of tasks should be processed while meeting specific design constraints. One of the most interesting subjects in this area is cipher breaking via brute-force attacks, which attracts the attention of many researchers to the field. In this paper, we introduce a novel exhaustive key search approach for block cipher cryptosystems. The key point is how to utilize the single instruction multiple thread architecture to improve the speed of the DES-like hardware-based cryptosystems. At first, the standard DES core is implemented while all operations like bit permutation, swapping, and general hardware data stream follow the original algorithm. Then, in order to maximize the usage of the memory bandwidth and to eliminate the bit access penalty in GPU architecture, we exploit the register permutation and swapping (instead of the conventional bit swapping) in our implementation. In this approach, each thread examines a set of 32 keys per each iteration and hence a considerable throughput is achieved. The experimental results demonstrate 24KX, 800X, and 400X speed up over the traditional DES implementation on single-core CPU, the best previous work on multi-core CPU, and the conventional implementation on GPU, respectively. Furthermore, we measure the power and energy consumption of the best GPU and CPU approaches, where the GPU implementation proves to be more power efficient.

Introduction

By the emergence of parallel high-throughput platforms, such as many-core GPUs and multi-core CPUs the software implementation of cryptography systems have become feasible and faster. Moreover, many researchers have proposed high-throughput software implementations for cryptography systems. However, due to programming difficulties these current software implementations fail to utilize the full capability of these days parallel platforms. In this work, we have utilized the bitslicing technique, which was previously used in the Eli Biham's DES encryption/decryption software implementation [2], in our own DES cryptanalysis software implementation. This way a number of 32 keys can be searched by each GPU thread, simultaneously.

This way, by having 32 keys processed simultaneously by each parallelization unit, we have achieved an unprecedented number of keys searched per second. This all happens while the bitscling technique adds no further memory overhead to the implementation. Moreover, each parallelization unit becomes capable of processing 32 keys in a fully parallel manner, which adds less overhead compared to a 32-iteration "for loop". The bitslicing technique achieves higher performance compared to the conventional implementations by increasing the amount of processed data while inhibiting the number of needed instructions from linear growth. The bitslicing representation technique is applicable to software implementation of systems that require multiple operations of bit granularity. In the case of the DES cryptanalysis, the bitslicing technique allows for the bit-level operations to happen in a much more efficient manner by utilizing the full Datapath width available in the aforesaid parallel platforms. Also, multiple bit-level shift and mask operations needed in the software implementation of the DES cryptanalysis methodology are done in the more efficient register-level swapping.

Challenges and Opportunities

Through our evaluations, we found that the bitslicing technique can be applicable to a wide range of applications for fully parallel SIMD execution. However, as can be seen, the integration and transformation of base instructions in most of applications to the bitsliced representation equivalents prove to be a burdensome task. Hence, we call on other researchers in other domains to use the proposed bitslicing technique to achieve a higher throughput compared to more conventional implementations. The bitslicing technique is a quite efficient way to achieve higher speed ups in data intensive operations and implementations. This bitslicing technique has also been successfully used in the fast AES encryption and decryption software implementation on GPU platforms [3].

References

[1] Ahmadzadeh, Armin, Omid Hajihassani, and Saeid Gorgin. "A high-performance and energy-efficient exhaustive key search approach via GPU on DES-like cryptosystems." *The Journal of Supercomputing* 74.1 (2018): 160-182.

[2] Biham, Eli. "A fast new DES implementation in software." *International Workshop on Fast Software Encryption*. Springer, Berlin, Heidelberg, 1997.

[3] Hajihassani, Omid, et al. "Fast AES Implementation: A High-Throughput Bitsliced Approach." *IEEE Transactions on Parallel and Distributed Systems* 30.10 (2019): 2211-2222.

Written on May 27, 2020