Master's Thesis Engineering Technology

2020-2021

Analysis and implementation of novel non-cryptographic hash functions

Thomas Claesen

Master of Electronics and ICT Engineering Technology

Objective

The goal of this Master's thesis is to design novel non-cryptographic hash functions based on reduced-round versions of the following symmetric-key ciphers: Speck, Pyjamask, GIFT, AES and Skinny. The number of rounds required are determined by the avalanche properties, while the timing properties determine the throughput.

Method

- Calculate the avalanche metrics of each cipher using python.
- Measure the number of rounds needed to satisfy the avalanche metrics.
- Implement the round-reduced hash functions using Vivado 2019.1 on three different FPGA platforms: Zynq 7020, Virtex Ultrascale and Virtex Ultrascale+
- Measure the maximum operating frequency of each non-cryptographic hash function either with or without key. See Figure 1.
- Measure the required number of resources at the maximum operating frequency for each hash function.
- Calculate the throughput of each hash function

Results

The results of the avalanche calculations are shown in Figure 2:

- 70-85% decrease in number of rounds needed.
- No difference between usage of key or not.

The timing results are shown in Figure 3:

- The utilization of the key has a significant negative impact on the operating frequency for Speck, Pyjamask and AES
- The Virtex boards are faster than the Pynq board, so the operating frequency is higher
- GIFT-NC shows the best performance out of all hash functions.

Figure 4 shows comparisons with existing hash functions:

- Our novel hash functions easily outperform the existing hash functions of Murmur3, FNV-1a and SipHash.
- Xoodoo-NC is slightly better in terms of performance than GIFT-NC.

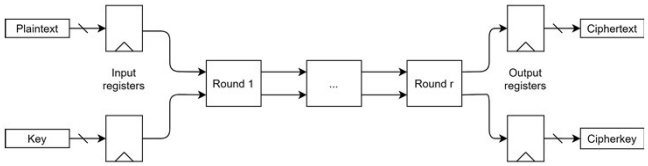

Figure 1: Implementation of the hash functions

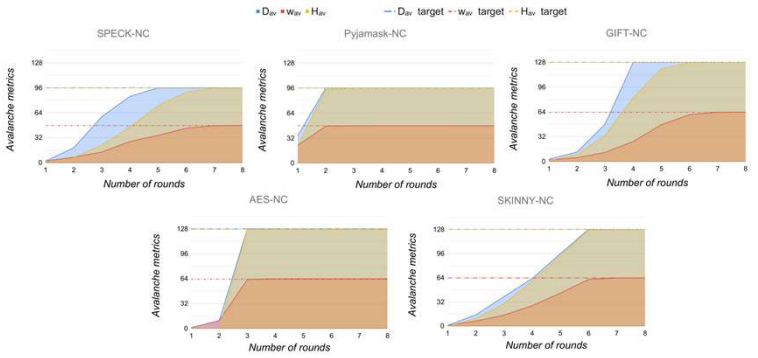

Figure 2: Results of the avalanche calculations

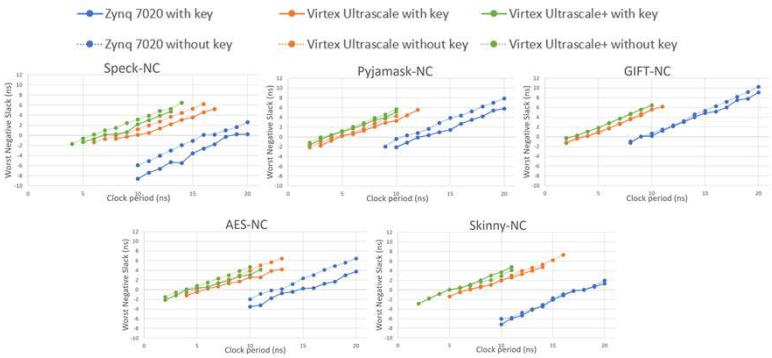

Figure 3: Results of the timing simulations

Hash function	Maximum frequency	Throughput (Mbps)	Tp / LUT (Mbps / LUT)	Delay (ns)
Murmur3	120.6 MHz	2,573	4.45	24.87
FNV-1a	122.9 MHz	925	1.63	130.08
SipHash [1]	182.8 MHz	1,463	1.38	21.88
Xoodoo-NC [2]	363.6 MHz	34,906	112.96	2.75
Speck-NC	166.66 MHz	16,000	37.04	6.000
Pyjamask-NC	250.00 MHz	24,000	29.59	4.000
GIFT-NC	333.33 MHz	32,000	58.61	3.000
AES-NC	250.00 MHz	24,000	10.79	4.000
Skinny-NC	200.00 MHz	19,200	8.82	5.000

Figure 4: Comparison with existing hash functions

Conclusion

The use of reduced round non-cryptographic versions of symmetric-key ciphers as hash functions show promising results in terms of throughput and avalanche metrics. Some hash functions, like GIFT-NC, perform better than others, but the other ciphers can be used as good alternatives if more than one hash function is needed for a given application.

Supervisors / Co-supervisors / Advisors

Prof. Dr. Ir. Nele Mentens
Dr. Ing. Jo Vliegen
Arish Sateesan

[1] D. G. L. Sekanina, "Fast Reconfigurable Hash Functions for Network Flow Hashing in FPGAs," in *NASA/ESA Conference on Adaptive Hardware and Systems*.

[2] A. Sateesan, J. Vliegen, J. Daemen and N. Mentens, "Novel Bloom filter algorithms and architectures for ultra-high-speed network security applications," in *23rd Euromicro Conference on Digital System Design*, 2020, pp. 262-269.

EMBEDDED SYSTEMS & SECURITY

UHASSELT

KU LEUVEN