FPGA Benchmarking Metrics

October 7, 2020

Metrics obtained from tool reports after placing and routing:

1. **Resource utilization**
   Number of LUTs (LEs for Cyclone 10LP) and flip-flops, assuming no use of embedded memories (such as BRAMs), DSP units, and embedded multipliers.
2. **Maximum clock frequency in MHz.**

Metrics calculated based on the execution time measurements (in clock cycles) obtained using functional simulation and the maximum clock frequencies (in MHz):

I. Throughput in Mbits/s

for the following sizes of inputs

a. long [with Throughput = d·Block size/(Time(N+d blocks)-Time(N blocks))]
b. 1536 bytes
c. 64 bytes
d. 16 bytes.

All throughputs calculated separately for

- authenticated encryption: AD, plaintext, AD+plaintext (sender's side)
- authenticated decryption: AD, ciphertext, AD+ciphertext (receiver's side), and
- hashing: hash message (both sides).

We assume no difference in the execution time depending on the result of verification on the receiver's side. A new key is assumed to be read and activated for each new input.

II. Speed in clock cycles per byte

This metric is suitable only for the case of a constant clock frequency determined by an application or implementation environment, independently of the maximum clock frequency supported by the LWC unit. Examples include RFIDs operating with the frequencies such as 60 kHz or 13.56 MHz. This metric is similar to the metric used in software benchmarking, but its use should be limited to the mentioned above special cases only. Otherwise, values of this metric may hide very significant differences in the maximum clock frequency, which in hardware is a strong function of an algorithm and hardware architecture.

III. Differences in the execution times for a new key and key reuse (in clock cycles)

This metric applies only to cores that allow reusing the same key for consecutive inputs. The differences in the execution times are typically constant. They can be measured experimentally using functional simulation.