Circuit Design for Security

Fabian Olbert

April 25, 2025

1 Performance Metrics

Further Readings: Digital Integrated Circuit Design – From VLSI Architectures to CMOS Fabrication; Cambridge University Press, 2008

1.1 Hardware Complexity

For ICs or **ASICs** the *area* of the logic is generally determined by the area in gate equivalents. 1GE is typically one NAND gate (2 PMOS + 2NMOS). The *memory* is determined by the amount of SRAM, DRAM, ROM...

For **FPGAs** the *area* is measured in slices. The unit to measure these area is the basic elements (Flip Flops, LUTs, DSP slices etc.) The *memory* is determined by the amount of distributed RAM (LUTs utilized as RAM) and the Block RAM.

1.2 Timing Related Performance

The *Critical Path Dealy* is proportional to the number of gates and the wire length in the longest path from one register to the next. It determines the maximum frequency.

The *Latency* is determined by the number of clock cycles required to perform the operation. There is a trade off between the critical path delay and the latency.

The *Throughput* is the amount of the processed data per processed time.

Assume there is a critical path with a path delay of 15ns.

f$_{max} = \frac{1}{15ns} \approx 66.67MHz(1)$

Example - Timing Related Performances

Assume Design with

- Latency $L = 1$

- Critical Path Delay (assume: incl. setup time, hold time, etc.): $d = 15ns$
- → Maximum frequency $f \approx 66.67MHz$
- → Throughput when "'processed data" = k:

$$throughput = \frac{k}{k \cdot 15ns} \approx 66.6 \cdot 10^6 \, \frac{\text{data}}{\text{s}}$$

Pipelining (put registers in logic path):

- Latency $L = 3$
- Critical Path Delay $d = 5ns$
- → Maximum frequency $f \approx 200MHz$
- → Throughput when "'processed data" = k:

$$\lim_{k\to\infty}(throughput) = \lim_{k\to\infty} \frac{k}{k \cdot 5ns + 10ns} = 200 \cdot 10^6 \, \frac{\text{data}}{\text{s}}$$