Suggested FPGA Design Goals
July 5, 2020

Highly recommended:

Maximum throughput, assuming

- 2000 or less LUTs
- 4000* or less FFs
- No BRAMs and no DSP units

of Xilinx Artix-7 FPGAs.

Optional:

1. Basic-iterative architecture
    a. Executing one round per clock cycle in block-cipher-based submissions
    b. Generating one output bit per clock cycle in stream-cipher-based submissions.
2. Architectures most natural for a given authenticated cipher, such as those based on
    a. Folding in block-cipher-based submissions
    b. Generating 2^d bits per clock cycle in stream-cipher-based submissions.
3. Maximum throughput, assuming
    - 1000 or less LUTs
    - 2000* or less FFs
    - No BRAMs and no DSP units

    of Xilinx Artix-7 FPGAs.
    Other limits, such as 1500 LUTs, 500 LUTs, etc. are welcome too.
4. Minimum latency, assuming
    - 2000 or less LUTs
    - 4000* or less FFs
    - No BRAMs and no DSP units

    of Xilinx Artix-7 FPGAs, for
    - Input composed of empty Associated Data and *n* bytes of plaintext, for *n*=16, 64, or 1536 bytes, processed using
        a) a new key
        b) the same key as the previous input.

Additional variants:

All of the above designs must support the AD, plaintext, ciphertext, and hash message sizes up to at least 2^{16}-1 bytes. The designers are *encouraged* to provide extended designs supporting the AD, plaintext, ciphertext, and hash message sizes up to at least

a. 2^{32}-1 bytes
b. 2^{50}-1 bytes,

with the

- negligible effect on the circuit maximum clock frequency, throughput, and latency
- minimum effect on circuit resource utilization.

* In modern Xilinx FPGAs, such as Artix-7 and Spartan-7, each LUT is accompanied by two FFs. This is because each LUT can be used to implement either an arbitrary combinational logic with 6 inputs and 1 output or an arbitrary combinational logic with 5 inputs and 2 outputs. For other targeted FPGA families, the numbers of FFs are the same as the numbers of LUTs, but LUTs can only be used to implement a combinational logic with 4 inputs and 1 output. As a result, the number of FFs will remain the same, while the number of LUTs will be substantially larger.