Timing - Romulus-N 1.3 Hardware Implementation

Aadam and Hawa Dirie

December 2021

Contents

Acronyms

cc Clock Cycles

m Number of Message Blocks (Plaintext or Ciphertext)

n Number of Associated Data Blocks

1 Key Setup Time

Key Setup Time = 4 Clock Cycles (cc)

2 Encryption Time

Encryption Time = $86 + (42*$ Number of Associated Data Blocks (n) $) + (46*$ Number of Message Blocks (Plaintext or Ciphertext) $(m)) + 4cc$

3 Decryption Time

Decryption Time = $86 + (42* \; n \;) + (46* \; m) + 8cc$

4 Message Authentication Time

4 cc (including loading tag from bdi) and 1 additional clock cycle for datapath to verify.
So answer is 5 cc

5 Time between two consecutive input blocks

42 cc

6 Throughput for long inputs as a function of the clock period

Assuming Throughput for large message =
(1/Minimum Clock Period) x (Bits/Block) /(cycles/Block)

6.1 Associated Data Blocks

$\frac{5376}{min\_clk\_period}$ bits per second

6.2 PlainText Blocks

$\frac{5888}{min\_clk\_period}$ bits per second

6.3 CipherText Blocks

$\frac{5888}{min\_clk\_period}$ bits per second

7 Confirmation through results

We were able to confirm through some preliminary testing of the datapath ciphercore and the use of for loops to determine the expected amount of time it took on average between each block of associated data and data blocks. The main difference being the additional 4 for data blocks due to the need of output of either ciphertext or plaintext depending on which mode one is in. Associated data blocks however do not have these extra 4 clock cycles as nothing is produced through bdi, only internal S register and other internal registers are modified.