Preliminary results of CryptoCliqIn

Experiment specification

Processor: Intel(R) Core(TM) i7-8650U CPU @ 190GHz 2.11GHz

Installed memory (RAM): 16.0

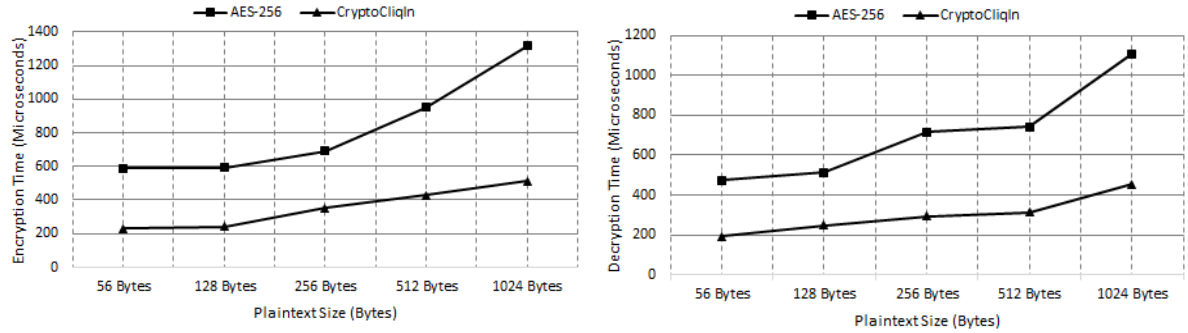
Operating System: Ubuntu 18.04.3 LTS (64 bits)

Programming: Python 3.7.8

Comparison Algorithm: AES-256 [1]

Results

The inputted plaintext size varies from 56 Bytes to 1024 Bytes to evaluate the *CryptoCliqIn* performance with different plaintext size. We run the simulation five times, and the average values of the results are listed in the following Figures and Tables. Tables are the real values plotted in Figure 1.



(a) Encryption time

(b) Decryption time

Figure 1: Comparison of CryptoCliqIn and AES-256 performance in the simulation platform

Table 1: Comparison of Encryption time (in microseconds) between AES-256 and CryptoCliqIn.

	56 Bytes	128 Bytes	256 Bytes	512 Bytes	1024 Bytes
AES-256	590.3636	594.1859	690.52837	951.2705	1316.2323
CryptoCliqIn	231.6498	243.6487	351.9420	428.8460	513.2696

Table 2: Comparison of Decryption time (in microseconds) between AES-256 and CryptoCliqIn.

	56 Bytes	128 Bytes	256 Bytes	512 Bytes	1024 Bytes
AES-256	474.5278	512.2945	717.13175	740.9945	1108.2298
CryptoCliqIn	191.9485	248.8745	295.8645	313.6832	453.7821

Reference

[1] AES python implementation: https://github.com/bozhu/aes-python