Performance Evaluation of Enhanced Encryption Scheme

In this report the proposed enhanced encryption scheme [1] is evaluated by its performance. Therefor, various tests will be performed in a simulated environment. As a weak block-cipher DES will be used and for encoding polar codes will be used. In this evaluation the new scheme will be compared with the lightweight pure DES encryption.

For each evaluation (test) random messages will be generated and compared after the decrypting. FThe following parameters are relevant for the evaluations:

Blocklength:
Blocklength (length of message) defines the size of block which will be encrypted. The encrypted message will be longer because of the polar encoding.

Erasure Rate:
Erasure rate (epsilon) defines the rate of erased bits in the simulated binary erasure channel. (An erasure rate of 0.25 would mean that 25% of the encoded word will be erased)

BEC Block:
Defines the size of the encoded block after the polar transformation.

The following parameters will be calculated based on the parameters above:

Infromation Bitrate:
The relation between information bits and parity bits. (Information bitrate of 0.5 and blocklength of 8 would mean 4 bits of parity and 4 bits of information. Information bitrate of 0.25 and a blocklength of 8 would mean 2 information bits and 6 parity bits)

$$\frac{blocklength}{bec\_blocklength}$$

Key Size:
Is 64 bits with DES

[1] A Security Enhanced Encryption Scheme and Evaluation of its Cryptographic Security

Encrypted Blocklength

The blocklength of the encrypted message

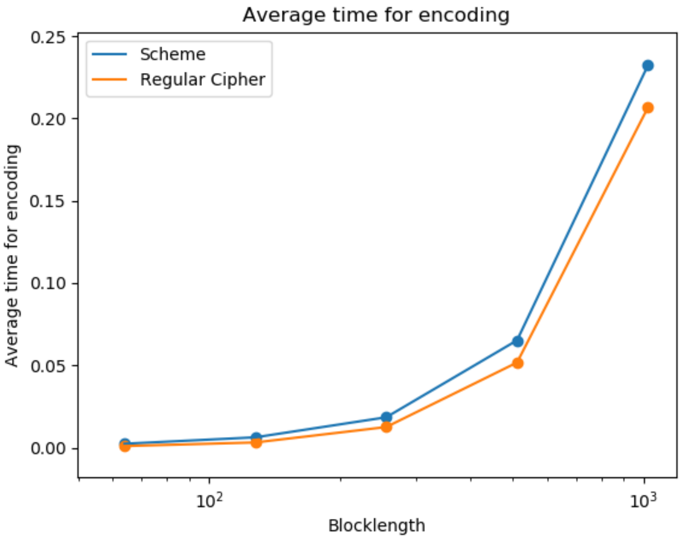
$$bec\_blocklength \cdot erasure\_rate$$

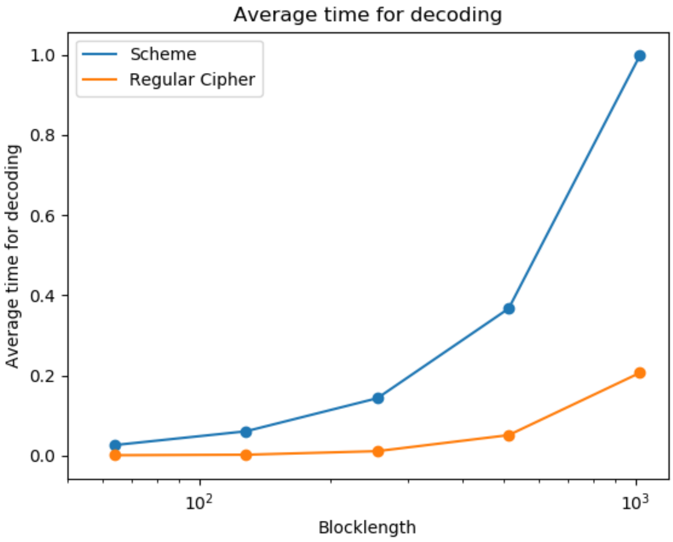
Comparison between Scheme and DES:

In this evaluation a simple performance comparison will made between the enhanced security scheme and DES. Blocklengths between 64 and 1024 bit will be evaluated.

Run 1:

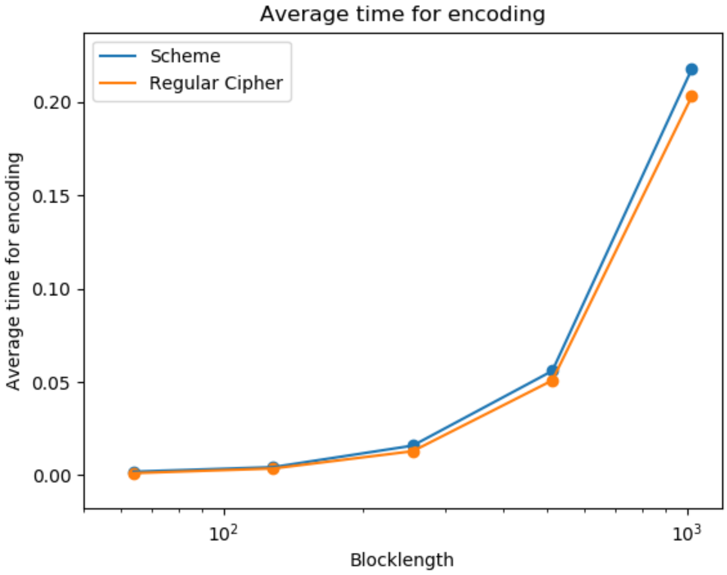
Erasure Rate:	0.25
Information Bitrate:	0.25

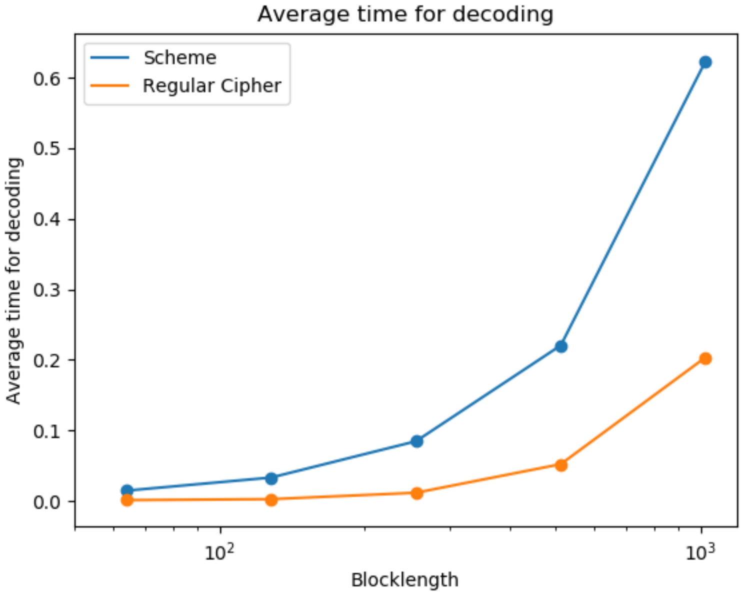




Run 2:

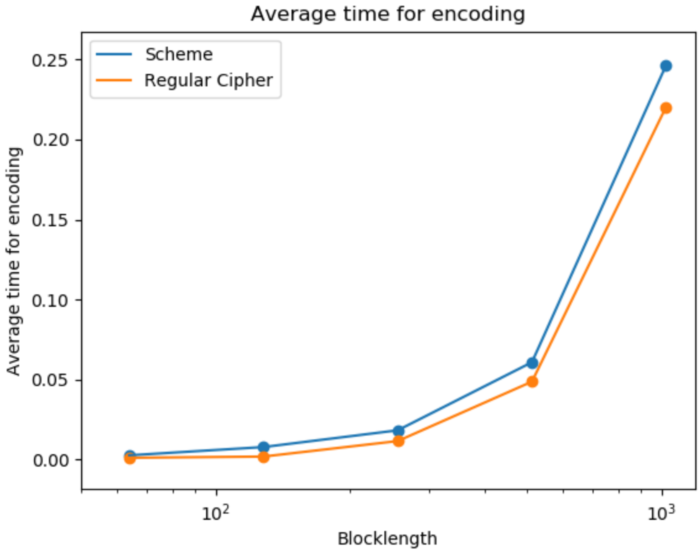
Erasure Rate:	0.25
Information Bitrate:	0.5

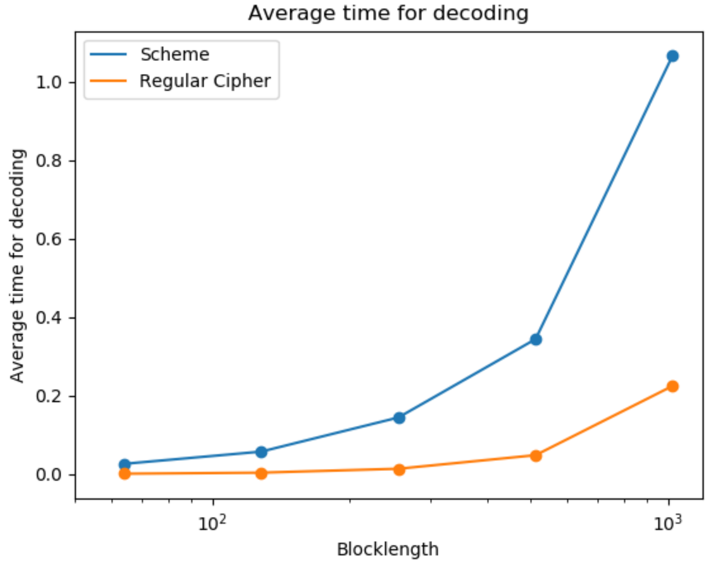




Run 3:

Erasure Rate:	0.5
Information Bitrate:	0.25



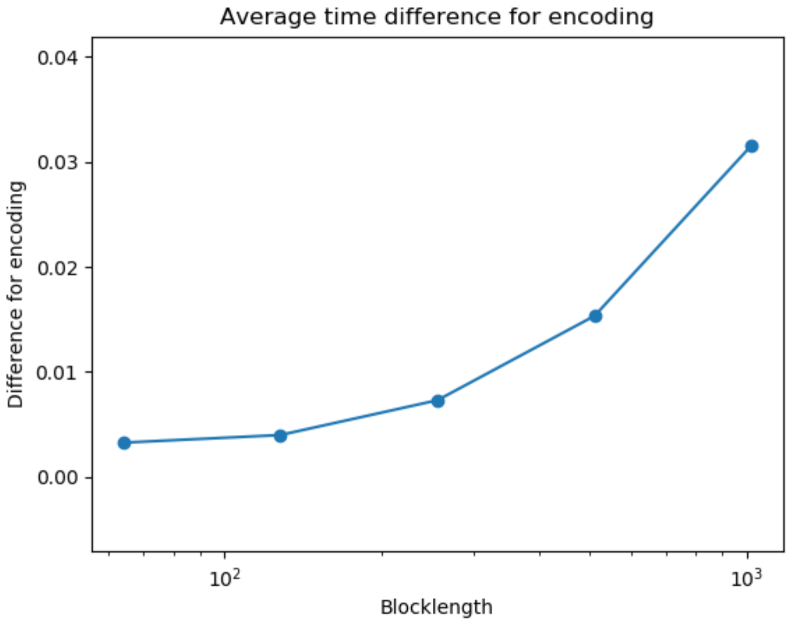


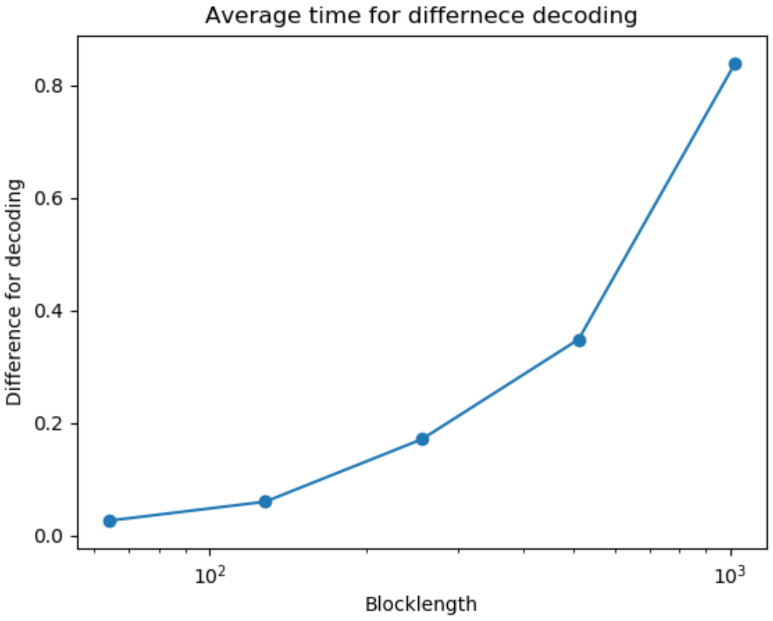
Execution Time Differences

In this evaluation the same tests as above will be performed and the execution-time difference between the enhanced cipher scheme and DES will be recorded. ($time\_scheme \ - time\_des$)
A new key will be generated after each iteration.

Run 1:

Erasure Rate:	0.25
Information Bitrate:	0.25

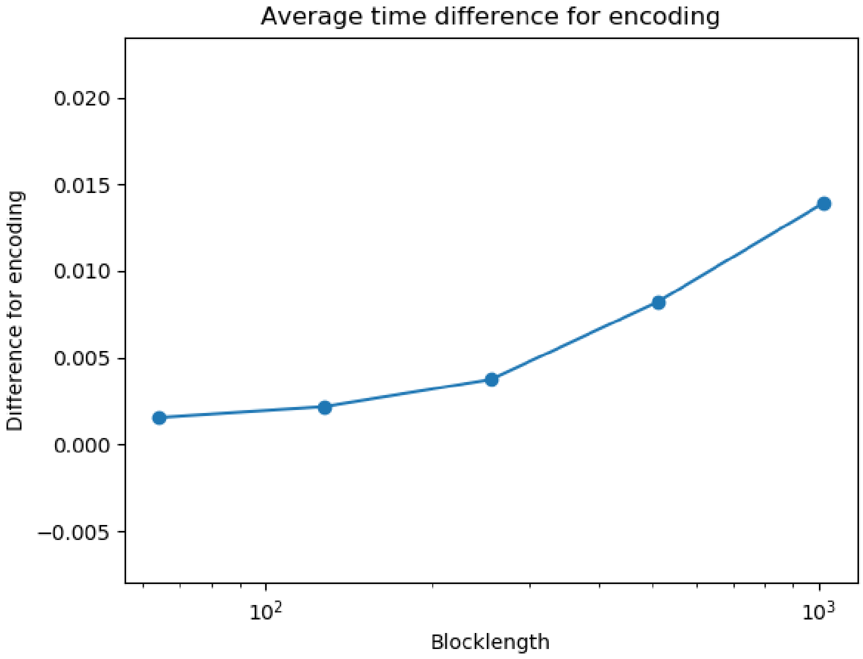


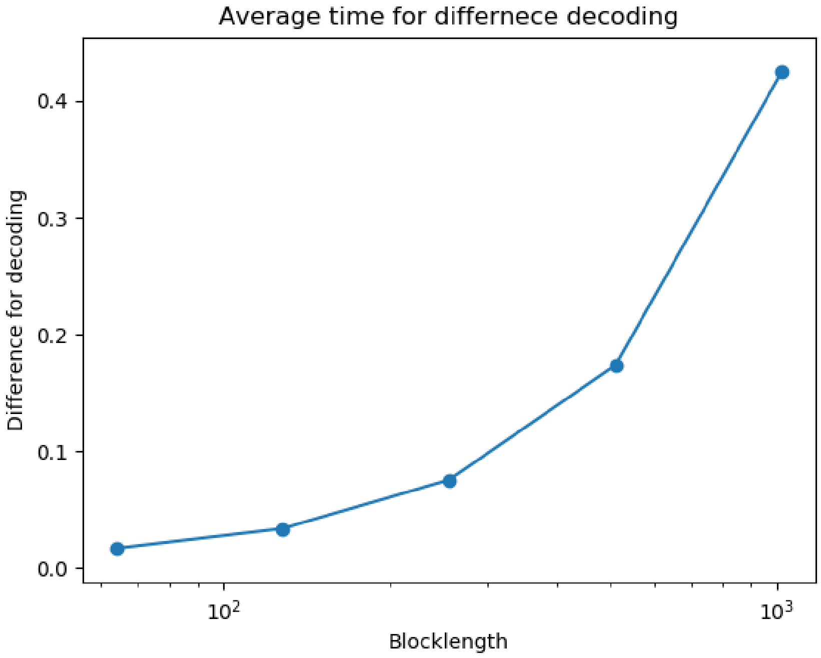


The time difference between the enhanced security scheme and DES increases linear with the blocklength.

Run 2:

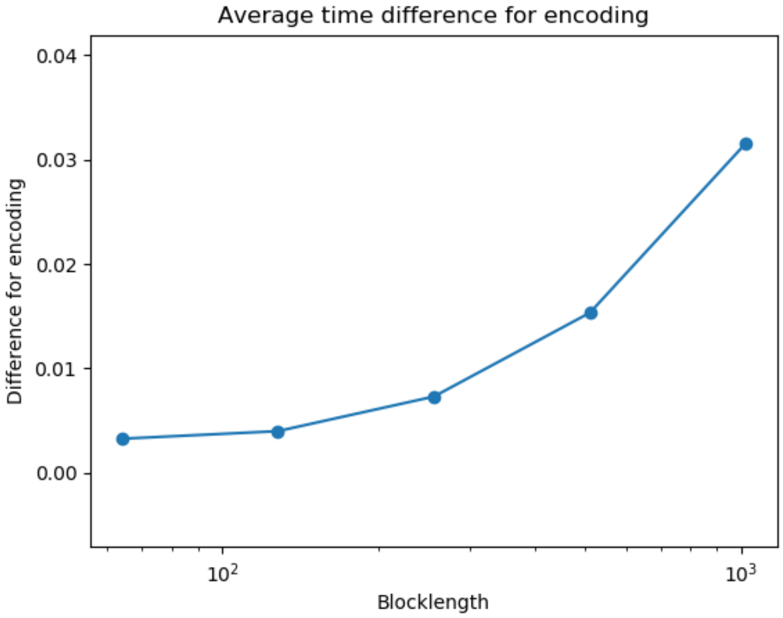
Erasure Rate:	0.25
Information Bitrate:	0.5

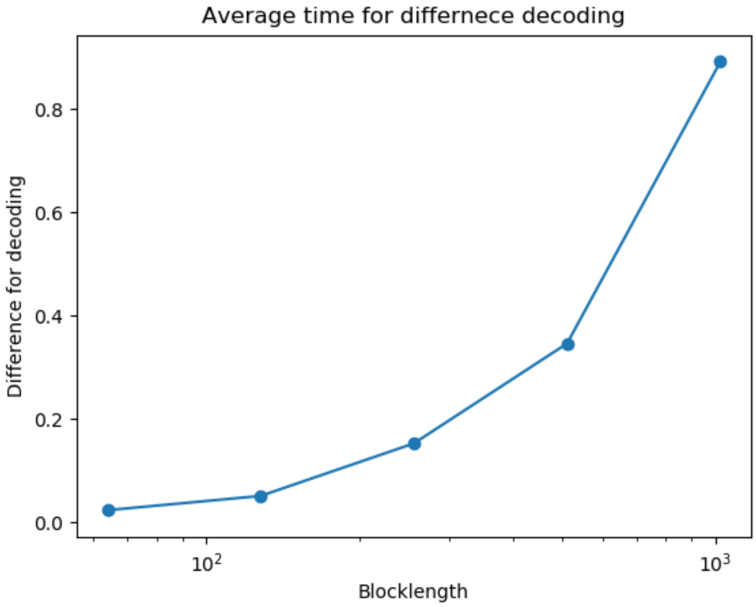




Run 3:

Erasure Rate:	0.5
Information Bitrate:	0.25





The same results can be observed here.

Normalized Time Complexity

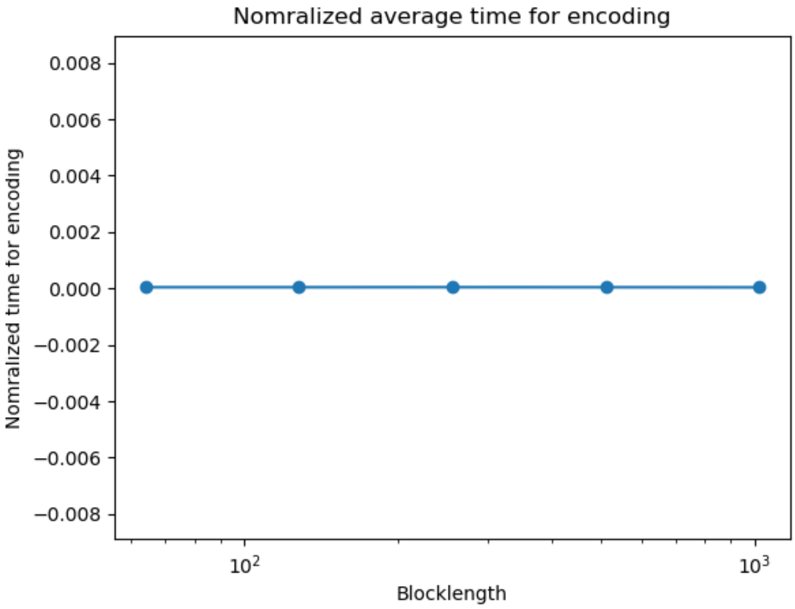
In this evaluation the same tests will be repeated, but the normalized time will be calculated. The following formula will be used to calculate the normalized time:

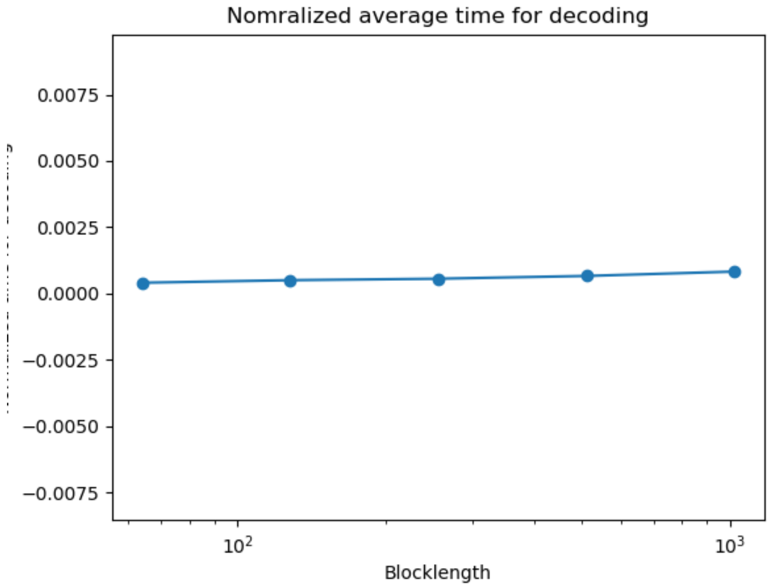
$$\frac{average\_time}{blocklength}$$

If the complexity if the enhanced security scheme is linear, the plot should show a steady flat line.

Run 1:

Erasure Rate:	0.25
Information Bitrate:	0.25

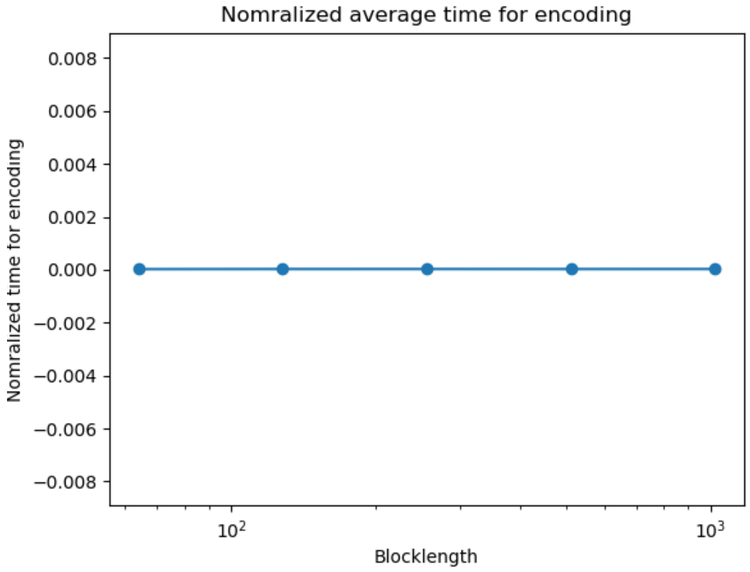


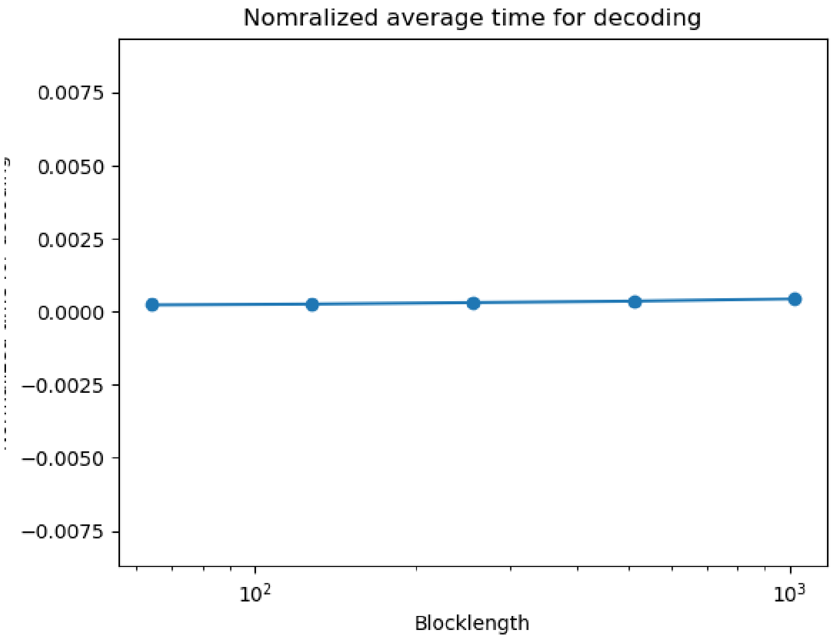


The normalized encoding time shows a flat line at 0 which proves, that encoding of the enhanced encryption scheme is linear to the blocklength. The decoding time shows a slight decrease. This shows that the decoding time per bit slightly increases with the blocklength. This can be explained by the large overhead in python, in order to simulate the decoding of the enhanced security scheme.

Run 2:

Erasure Rate:	0.25
Information Bitrate:	0.5





The increase in decoding is 50% less by increasing the information bitrate from 0.25 to 0.5.

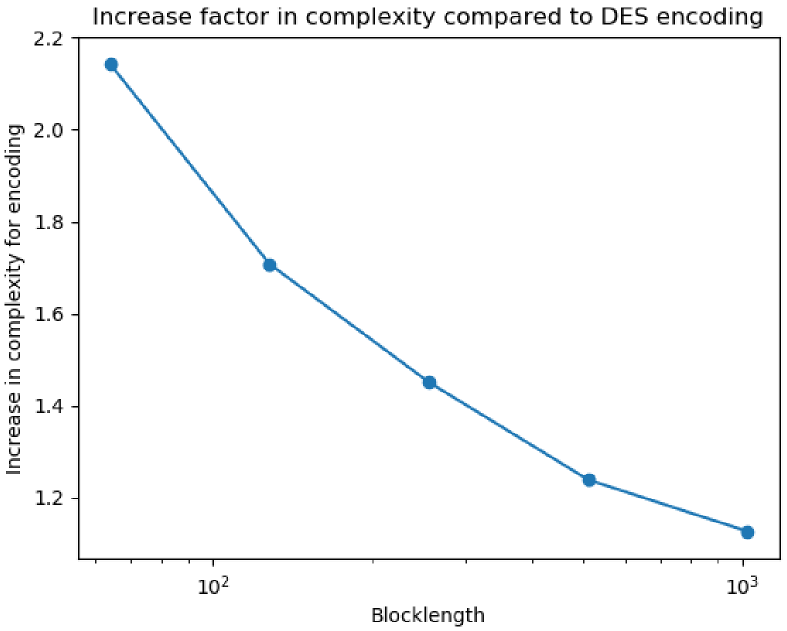
Time Complexity Increasing Factor

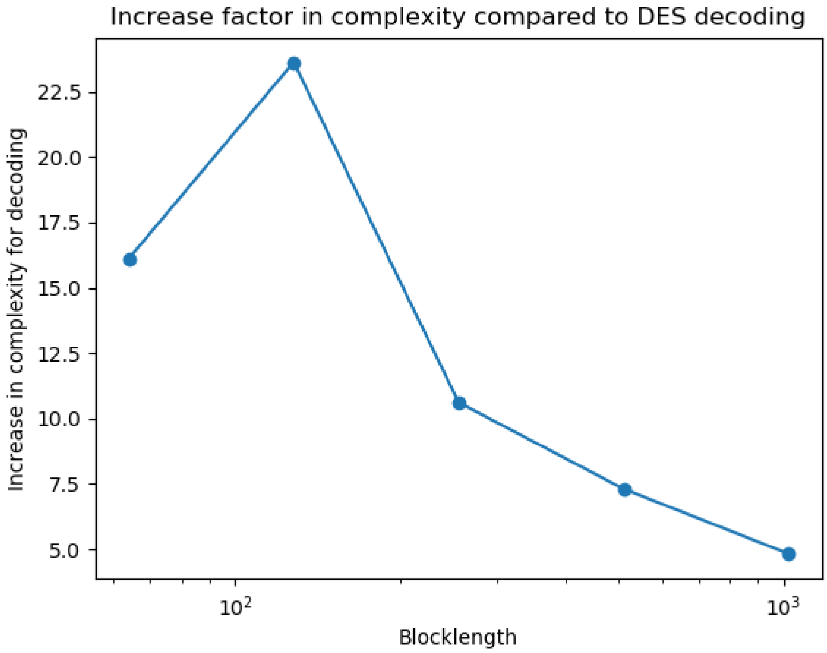
In this evaluation the increasing factor in complexity will be compared from DES to the enhanced cipher scheme. The following formula will be used for the plots:

$$\frac{time\_scheme}{time\_des}$$

Run 1:

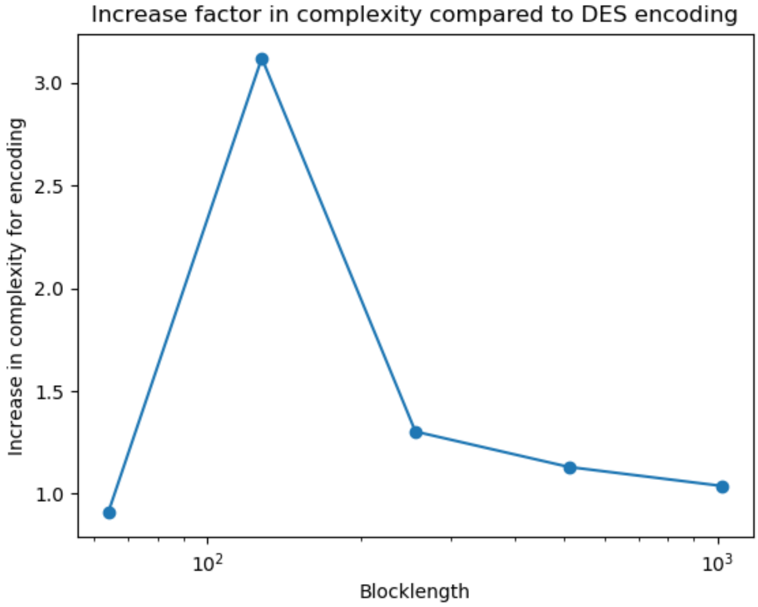
Erasure Rate:	0.25
Information Bitrate:	0.25

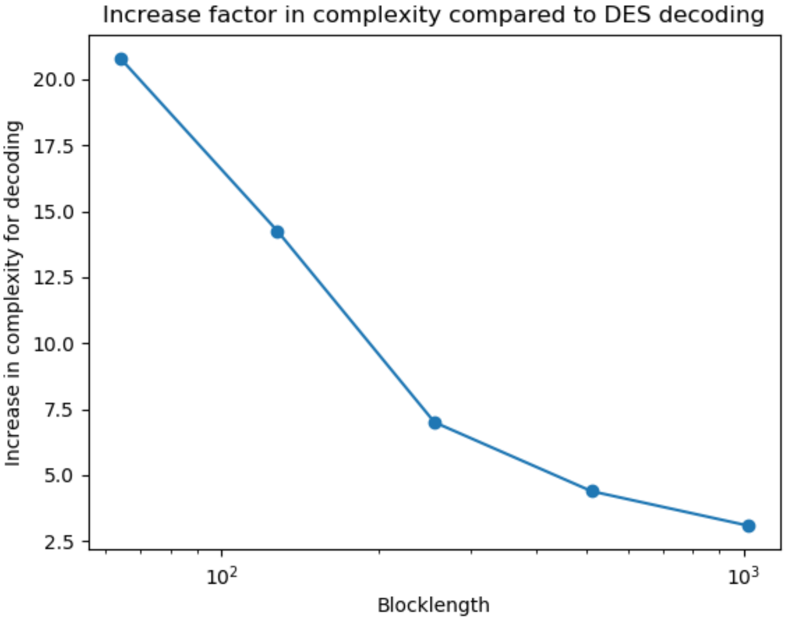




Run 2:

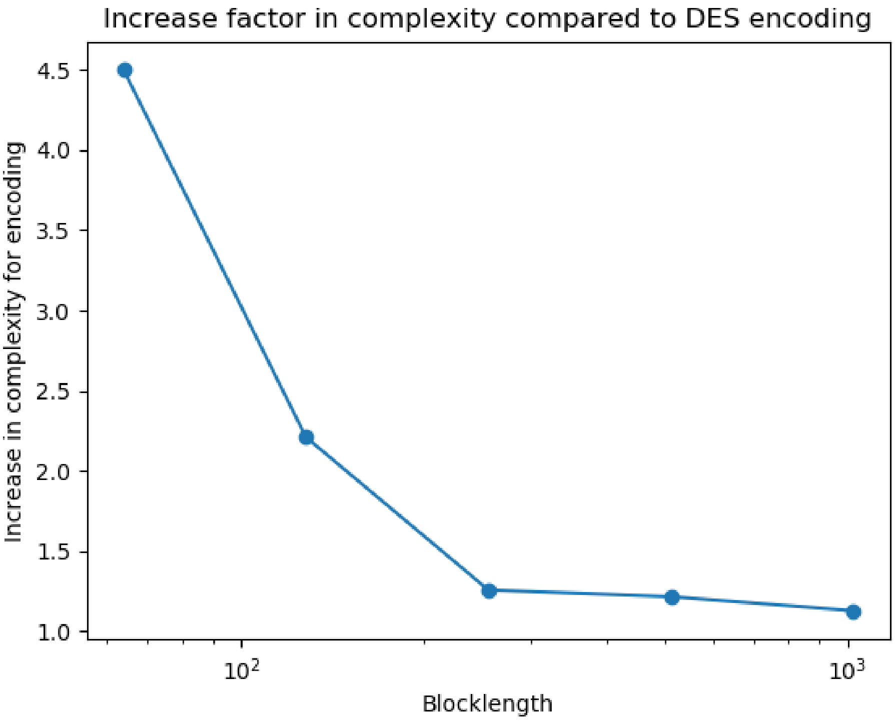
Erasure Rate:	0.25
Information Bitrate:	0.5

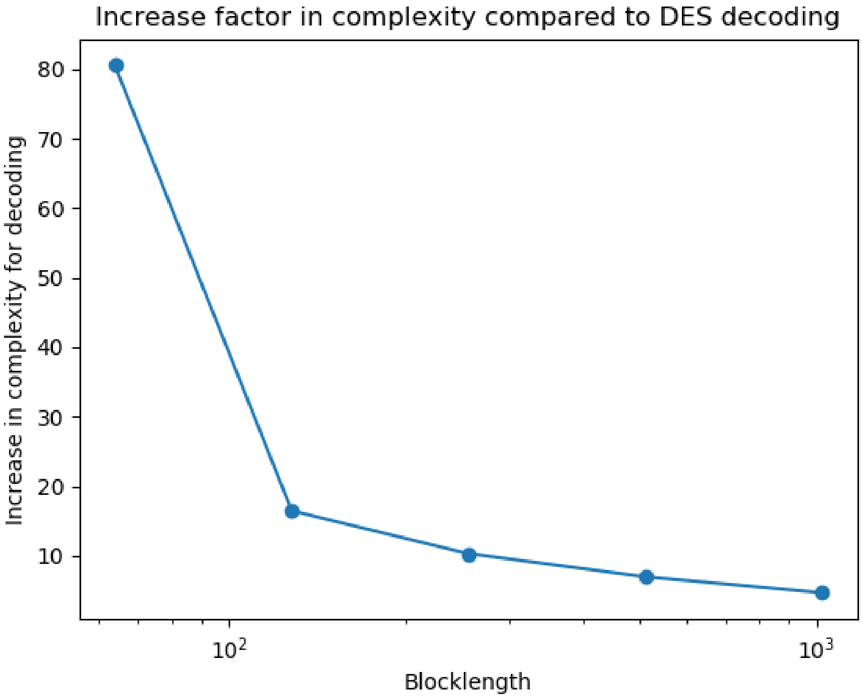




Run 3:

Erasure Rate:	0.5
Information Bitrate:	0.25


Increase factor in complexity compared to DES encoding
Increase in complexity for encoding
10^2
10^3
Blocklength


Increase factor in complexity compared to DES decoding
Increase in complexity for decoding
10^2
10^3
Blocklength