Quantum Safe Crpytography

A Report Submitted
in Partial Fulfillment of the Requirements for
the Degree of
Bachelor of Technology
in
Computer Science & Engineering

by
Golu Kumar(20174024)
Adarsh Awasthi(20174015)
Ashish Patel(20174006)

to the

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT MOTILAL NEHRU
NATIONAL INSTITUTE OF TECHNOLOGY ALLAHABAD, PRAYAGRAJ
May, 2021

UNDERTAKING

I declare that the work presented in this report ti- tled "Quantum Safe Cryptography", submitted to the Computer Science and Engineering Department, Motilal Nehru National Institute of Technology Allahabad, Prayagraj, for the award of the ***Bachelor of Technology*** degree in ***Computer Science & Engineering*** , is my original work. I have not plagiarized or submitted the same work for the award of any other degree. In case this undertaking is found incorrect, I accept that my degree may be unconditionally withdrawn.

May, 2021 Allahabad

(Golu ,Adarsh,Ashish)

_____

CERTIFICATE

Certified that the work contained in the report titled “Quantum Safe Cryptography”, by group CS-41, has been car- ried out under my supervision and that this work has not been submitted elsewhere for a degree.

DR ANOJ KUMAR
(Guide Name)
Computer Science and Engineering Dept.
M.N.N.I.T Allahabad, Prayagraj

May, 2021

Preface

A good B.Tech. thesis is one that helps you in furthering your interest in a specific field of study. Whether you plan to work in an industry or wish to take up academics as a way of life, your thesis plays an important role.

Your thesis should judiciously combine theory with practice. It should result in a realization of reasonably complex system (software and/or hardware). Given various limitations, it is always better to extend your predecessor's work. If you plan it properly, you can really build on the experience of your seniors.

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to our mentor and guide Dr. Anoj sir for bringing us the opportunity of exploring a rising research area in modern quantum safe cryptography algorithms.

We are heartily obliged to our panel mentors and the open environment of knowledge sharing between our colleagues.

All the suggestions and critics for the further development of the ideas are welcome.

Team CS-41
Golu Kumar
Adarsh Awasthi
Ashish Patel

==========

Contents

Preface

Acknowledgements

1 Introduction

2 Related Work

3 Proposed Work

4 Experimental Setup and Results Analysis

5 Conclusion and Future Work

6 A Some Complex Proofs and simple Results

References

CHAPTER –1

INTRODUCTION

Characteristics of Algorithm

1 **A 128 BIT SYMMETRIC BLOCK CIPHER**

2 **KEY LENGTH OF 128-192 AND 256 BITS**

3 **NO WEAK KEY**

4 **128 BIT BLOCK FEISTEL NETWORK**

5 **16 ROUND AND PRE AND POST WHITEN-ING**

6 **KEY DEPENDENT S BOXES**

7 **FLEXIBLE DESIGN**

8 **SIMPLE DESIGN**

9 **KEY SCHEDULE COMPUTABLE ON THE FLY**

CHAPTER –2

RELATED WORK

1. Confusion - There should be minimal obvious relationship between plaintext,key and cipher
2. Diffusion - Every bit of cipher should depend on every bit of plaintext and every bit of the key

These two concepts and independence of feistel architecture from the round function makes basis of our algorithm. The "keys" and matrices are inspired from the ongoing research in coding theory.

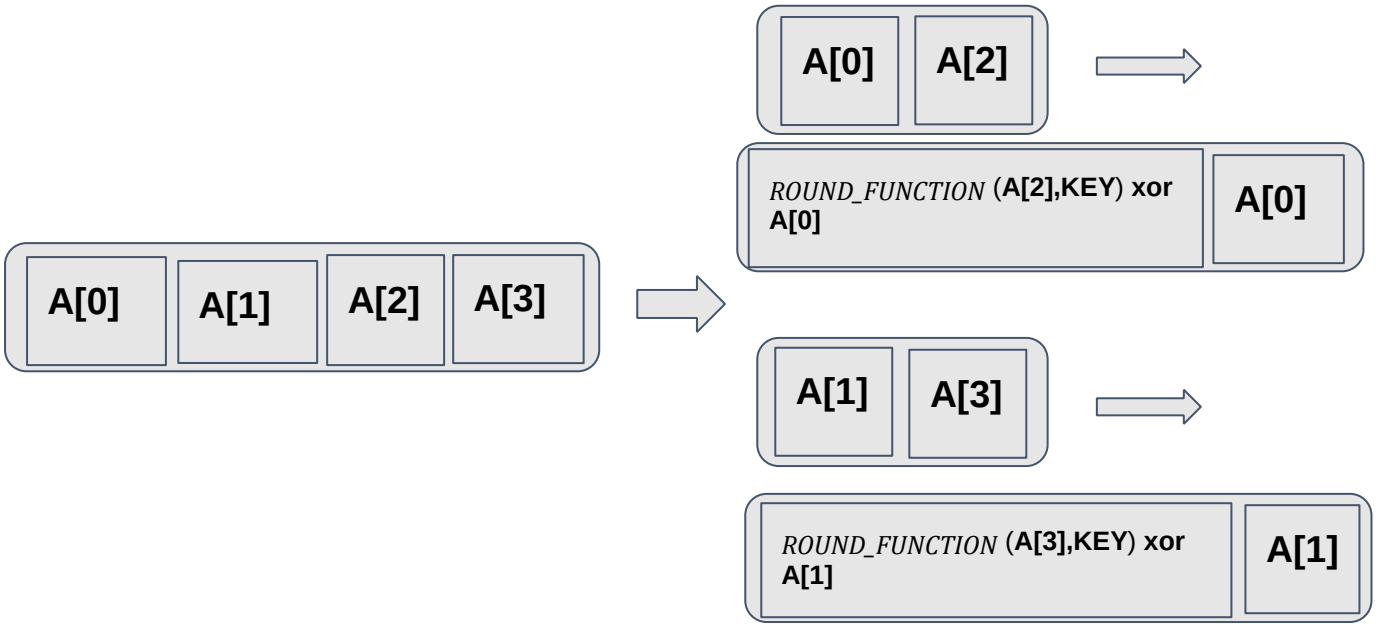
CHAPTER –3

PROPOSED WORK

The project is about designing a variation of a quantum safe algorithm. The algorithm which should take apparently enough time to be broken by brute force attack even with the help of Qbit computer processing power.

● **NORMAL FEISTEL CIPHER**

● **MODIFIED FEISTEL CIPHER in our project**



The methodology of the Error correcting codes:

Let us suppose that we want to transmit a 3 bit data: “010”, but instead of sending this as it is,

I will send “000 111 000” instead , such that if in future it gets polluted to be something like “010 110 001” , then we can retrieve the original data by taking maximum occurring bit from each of the chunk of the three.

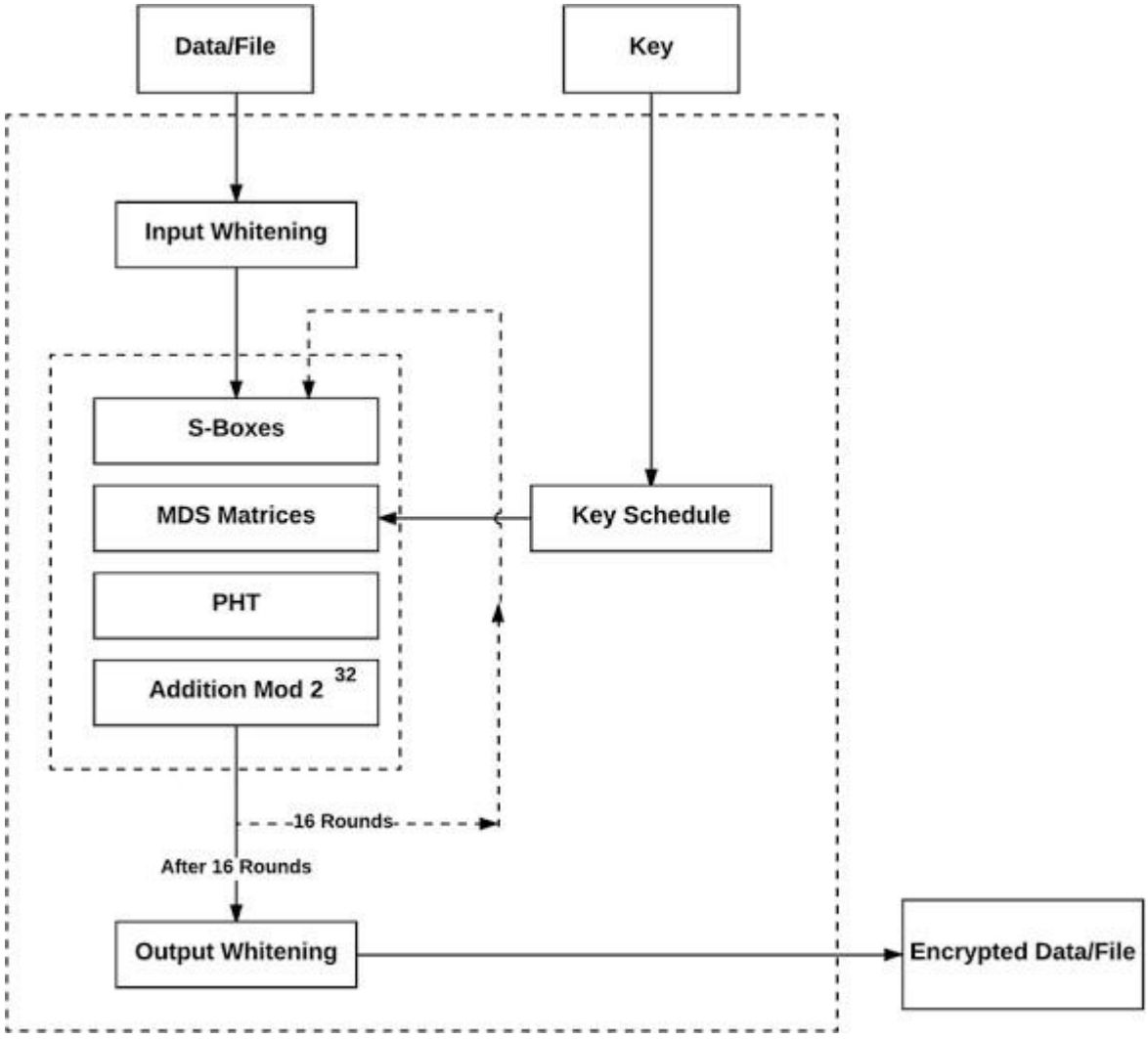
Now we learn that if we have a bit pattern of length of “N” then we can convert it into a corresponding sequence of length of “M” such that M=cN, which will make the process of correction easier only on encryption and decryption side but the transmitted data will not be the same plaintext.

Finally we have sequence to be sent as : “001”
I can convert them into either “000 000 111” or “010 001 110”, because both of them will be producing the same pattern when we will run selection based on majority of frequency.

SO, we have used the Maximum Distance Separable(MDS) matrix for modifying the original plaintext to new plaintext which will go for the further encryption process by linear transformation.

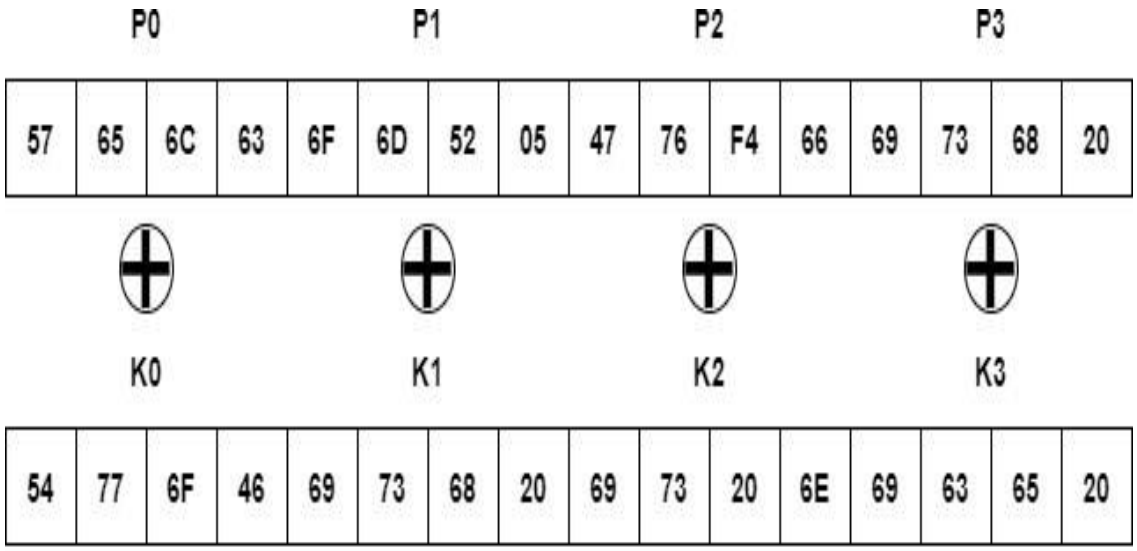
MDS will corrupt the text but will keep the original information safe as the process of the maximum frequency method can extract the codes after the decryption process.

The Algorithm:-



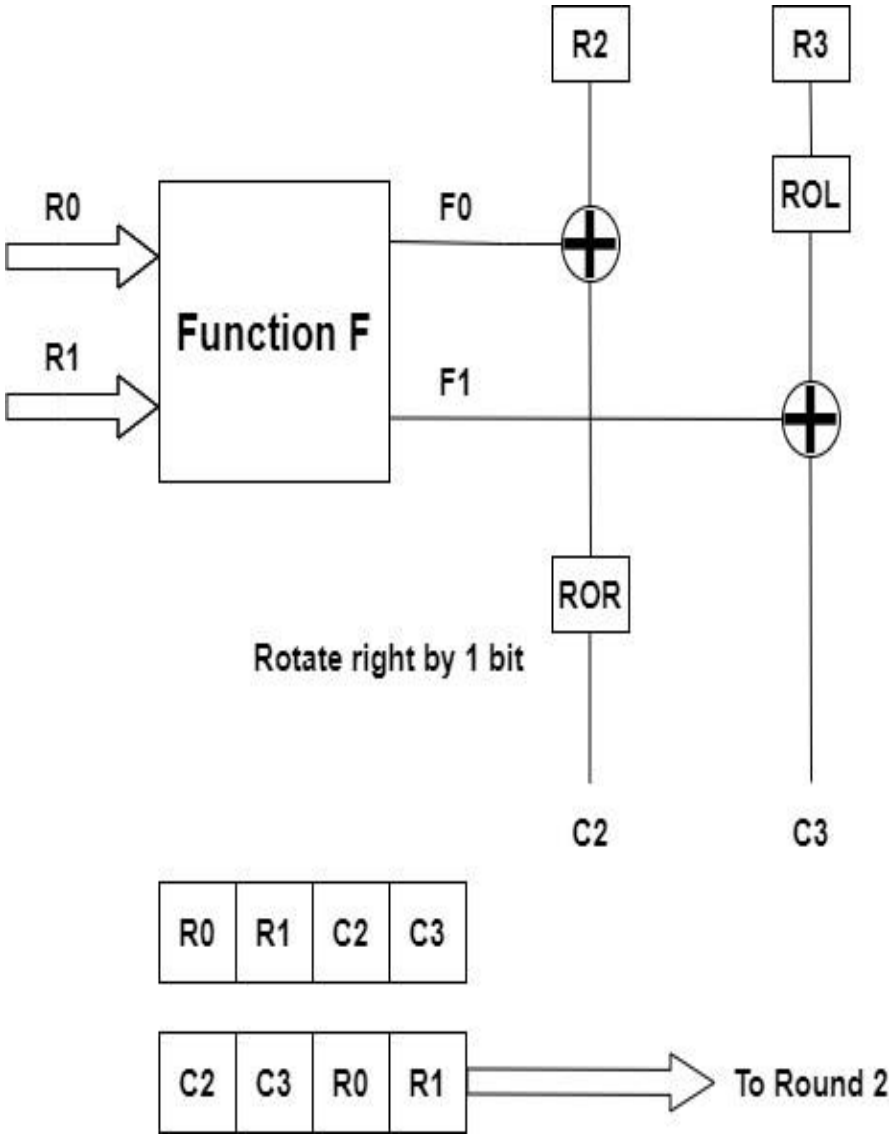
16 Rounds
Input Whitening:-

128 bit plain text (divided into four parts of 32 bits each) is given for the input whitening where it is xor-ed with four keys

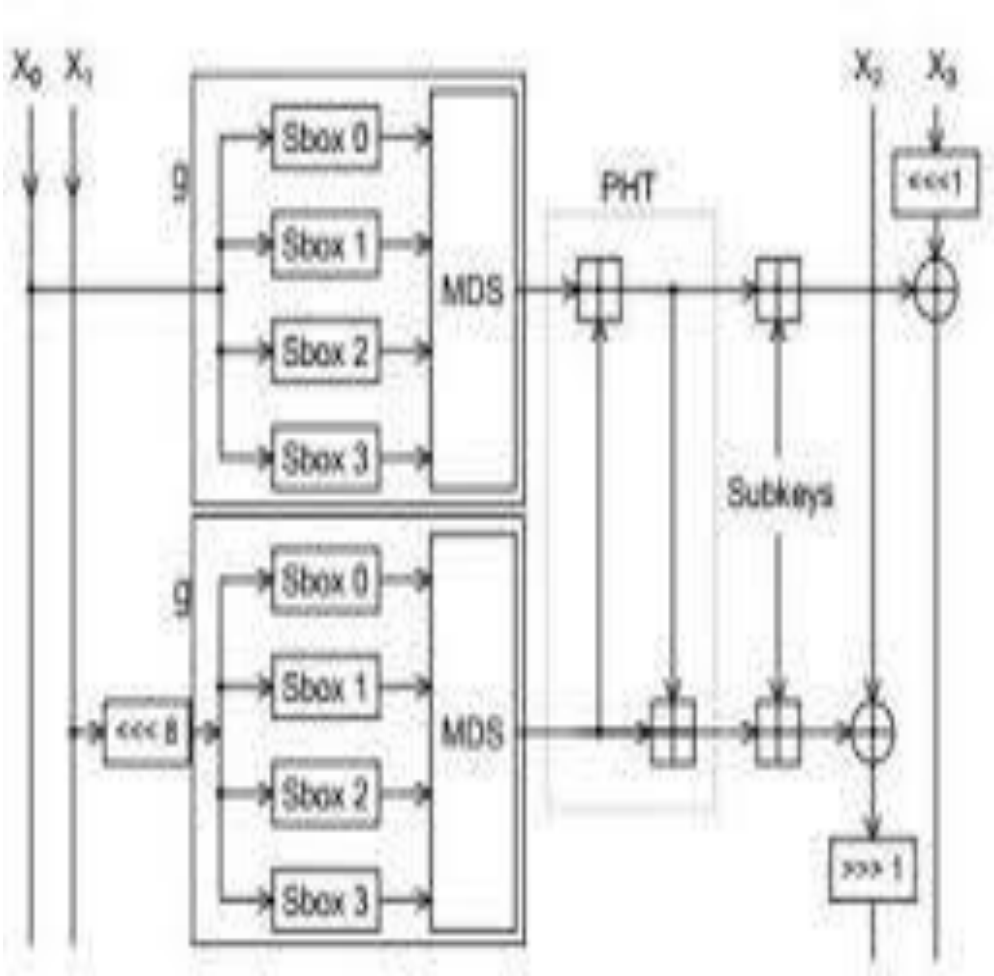


03	12	03	25	06	1E	3A	25	2E	05	D4	08	00	10	0D	00

At this point the result words R0,R1,C2,C3 are final results of round 1 but before sending the four words to round 2 we need to swap them.
Two fish has 16 rounds in total. This is result of first round.


R2
R3
ROL
R0
F0
Function F
R1
F1
ROR
Rotate right by 1 bit
C2
C3
R0
R1
C2
C3
C2
C3
R0
R1
To Round 2

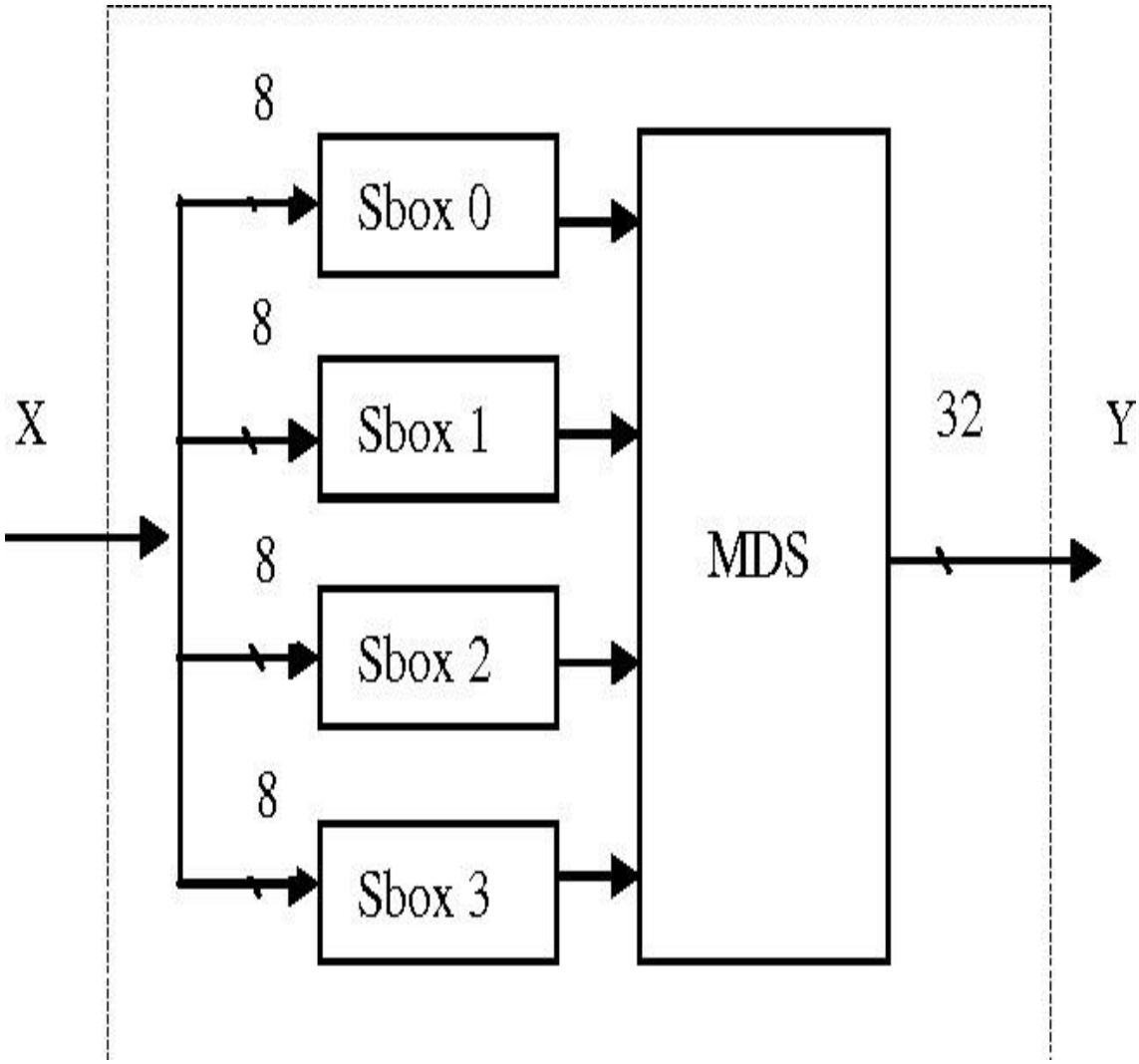
Function F



Function G:-

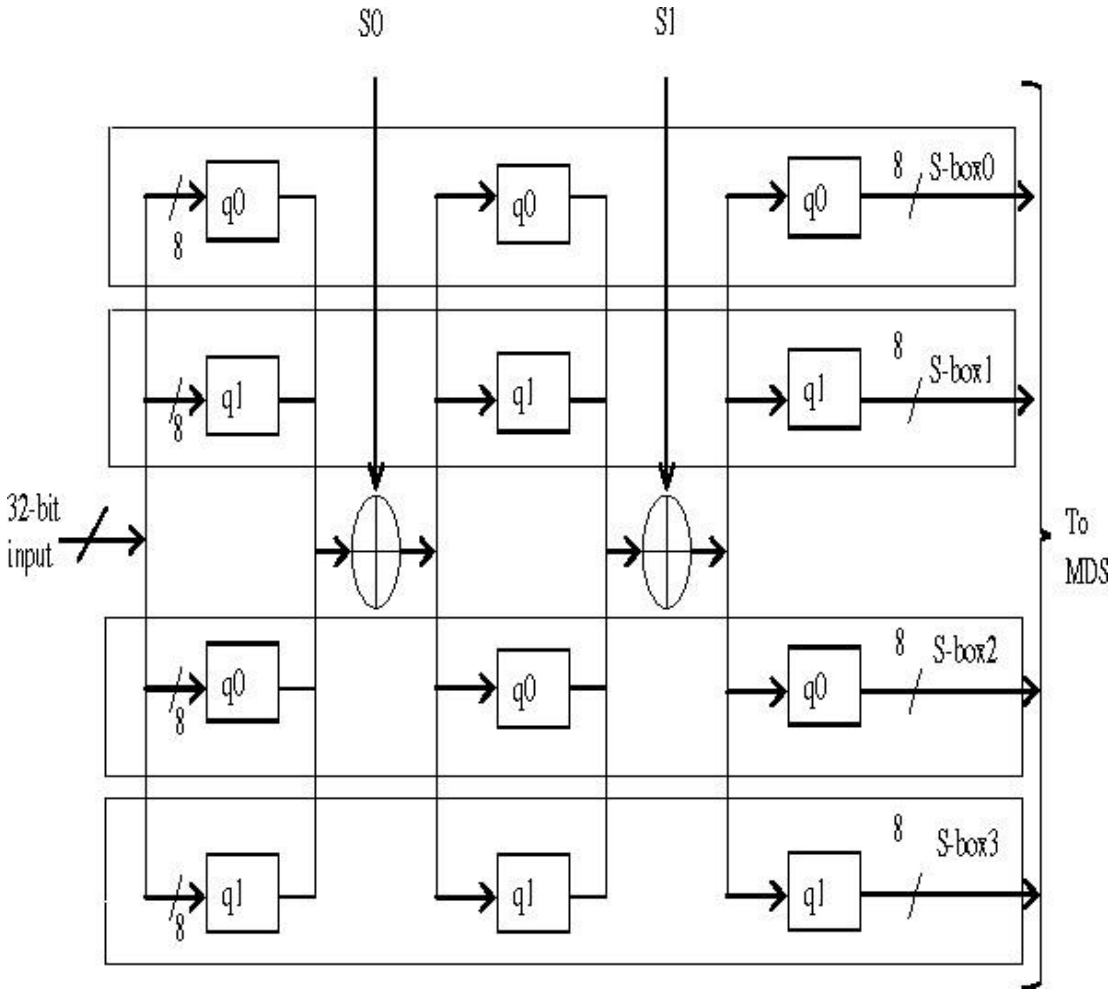
The function G forms the heart of Two Fish. The in- put X is split into four bytes. Each byte is run through its own Key-dependent S-Box. Each S-Box takes 8 bit

of input and produces 8 bit of output.



The four results are interpreted as a vector of length 4 over GF(2^8). The resulting vector is interpreted as 32 bit word which is result of G.

S-Box



Each S-Box consists of three 8-by-8-bit fixed permutations chosen from a set of two possible permutations of q0 ad q1.
Between these three permutations XOR operations are performed with subkeys S0 and S1.
These subkeys are computed only once for a particular global key and stay fixed during the entire encryption and decryption process.

CHAPTER –5

CONCLUSION AND FUTURE WORK

Conclusion:

We studied a variation of algorithms which participated in the NIST standard Cipher competition in 2019 and tried to re-invent the algorithm with the help of an emerging branch of problem solving mathematics i.e. coding theory.We completed the algorithm design and are progressing towards the efficient implementation of the algorithm.

Future work:

Today most of the implemented algorithms are lightweight cryptography algorithms because they are developed on IoT . After discussion with teammates and our mentor , we decided to extend this project and make this algorithm suitable for IoT devices.

CHAPTER –6

SOME COMPLEX PROOF AND RESULTS

- **the function "F": (input=R$_0$,** $R_1//32bit\ each$) =>

  $T_0 = g(R_0)$

  $T_1 = g(ROL(R1, 8))$

  $F_0 = (T_0 + T\,1 + K_{2r+8})\ mod\ 2^{32}$ F_1

  $= (T_0 + 2 * T\,1 + K_{2r+9})\ mod\ 2^{32}$

- **the function "g": (input=R$_0$**$//32bit$) =>

  $X_0 = R$ & ((1 << 8) − 1)

  $X_1 = X_0$ & ((1 << 8) − 1)

  $X_2 = X_1$ & ((1 << 8) − 1)

  $X_3 = X_2$ & ((1 << 8) − 1)

  => $Y_0 = S_0(X_0)$, $Y_1 = S_1(X_1)$, $Y_2 = S_2(X_2)$

  $Y_3 = S_3(X_3)$ $NOTE$: [S_0, $S1$...$are\ S\ boxes$] => F

  = [F_0, F_1, F_2, F_3] = [$MDS\ Matrix$][Y]

- **the "S box"=(input=X// 8 bit)**

  S-box contains a permutation of size=3 made up of 2 functions q$_0$ $and\ q_1$.

let's say sequence is S$_0$ = [q_0, q_1, q_0], $S1$ = [$q1$, $q0$, $q0$], $S2$ = [q_1, q_1, q_0], $S3$ = [q_1, q_0, q_0] **When going through qi series of function the input to function "g" are XORed with Schedule keys S0 and S1 and finally transferred to MDS matrix for input.**

- **the function "q_i"** : ($input = x//8bit$) => a_0; $b_0 = x/16$; $x \; mod \; 16$ $a_1 = a_0 \; xor \; b_0$
  $b_1 = a_0 \; ROR4(b_0; 1)$ $8a_0 \; mod \; 16$
  a_2; $b_2 = t_0[a_1]$; $t_1[b_1]$ $a_3 = a_2 \; xor \; b_2$
  $b_3 = a_2 \; ROR4(b_2; 1)$ $8a_2 \; mod \; 16$
  a_4; $b_4 = t_2[a_3]$; $t_3[b_3]$
  $y = 16 \; b_4 + a_4$
- **The MDS matrix is made up of stan- dard MDS suggested by coding theory problem.**
- **Key schedule: The key schedule is in- spired from the twofish encryption ar- chitecture**

1. **Keys for input and output whitening = 4**
2. **Keys for 16 rounds=16**
3. **Keys for S-Box scheduling = 2**

TOTAL KEYS=22

NOTE : we need to perform output whitening as well at the end of decryption using same whiten- ing key-set used for encryption purpose.

REFERENCES

1. https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancingpost-quantum-crypto-semifinals
2. https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf
3. https://en.wikipedia.org/wiki/Coding_theory#:~:text=Coding%20theory%20is%20the%20study,data%20transmission%20and%20data%20storage.