Kalyna

Lock N Load

Department of EECS
Indian Institute of Technology Bhilai

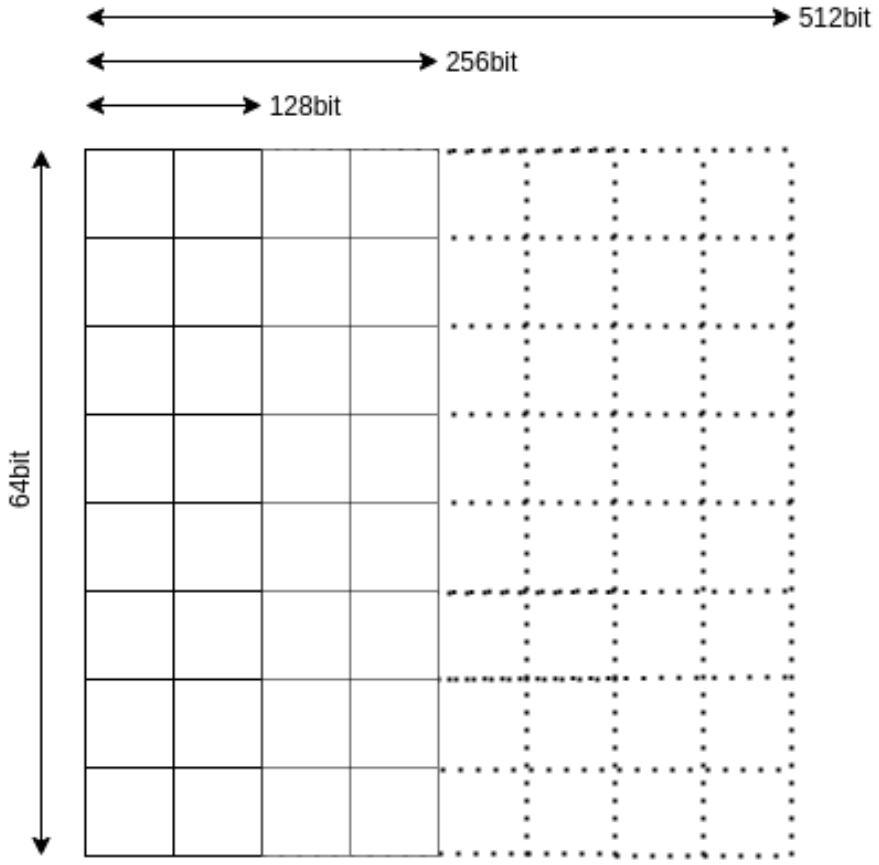
November 27, 2020

Outline

Supported block and key length

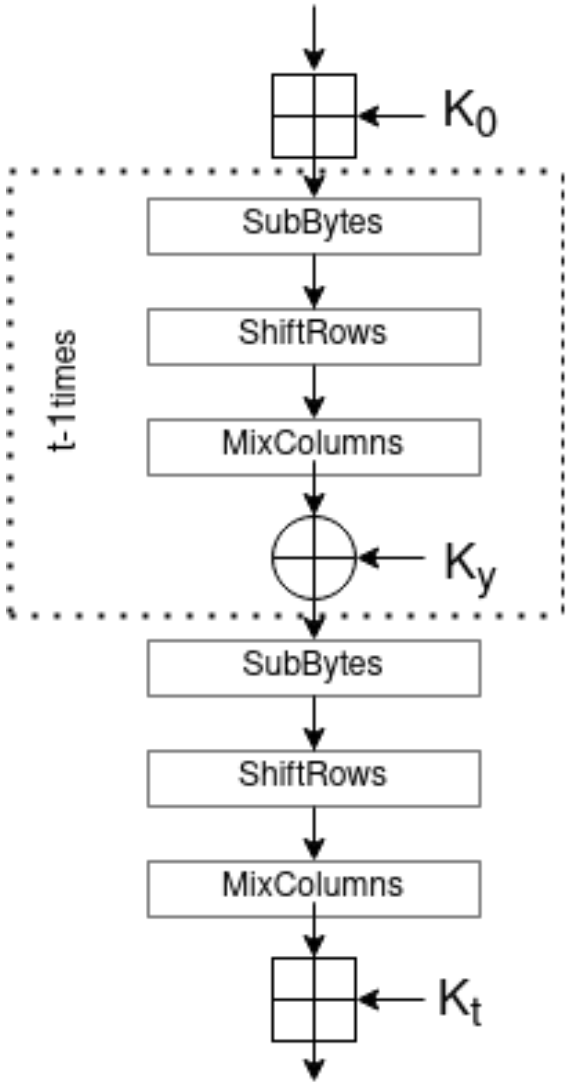
#	Block Size	Key Length	Rounds
1	128	128	10
2	128	256	14
3	256	256	14
4	256	512	18
5	512	512	18

About State



- Each cell contains 1Byte
- Matrix is filled Top to Bottom and Left to Right

Brief overview of structure

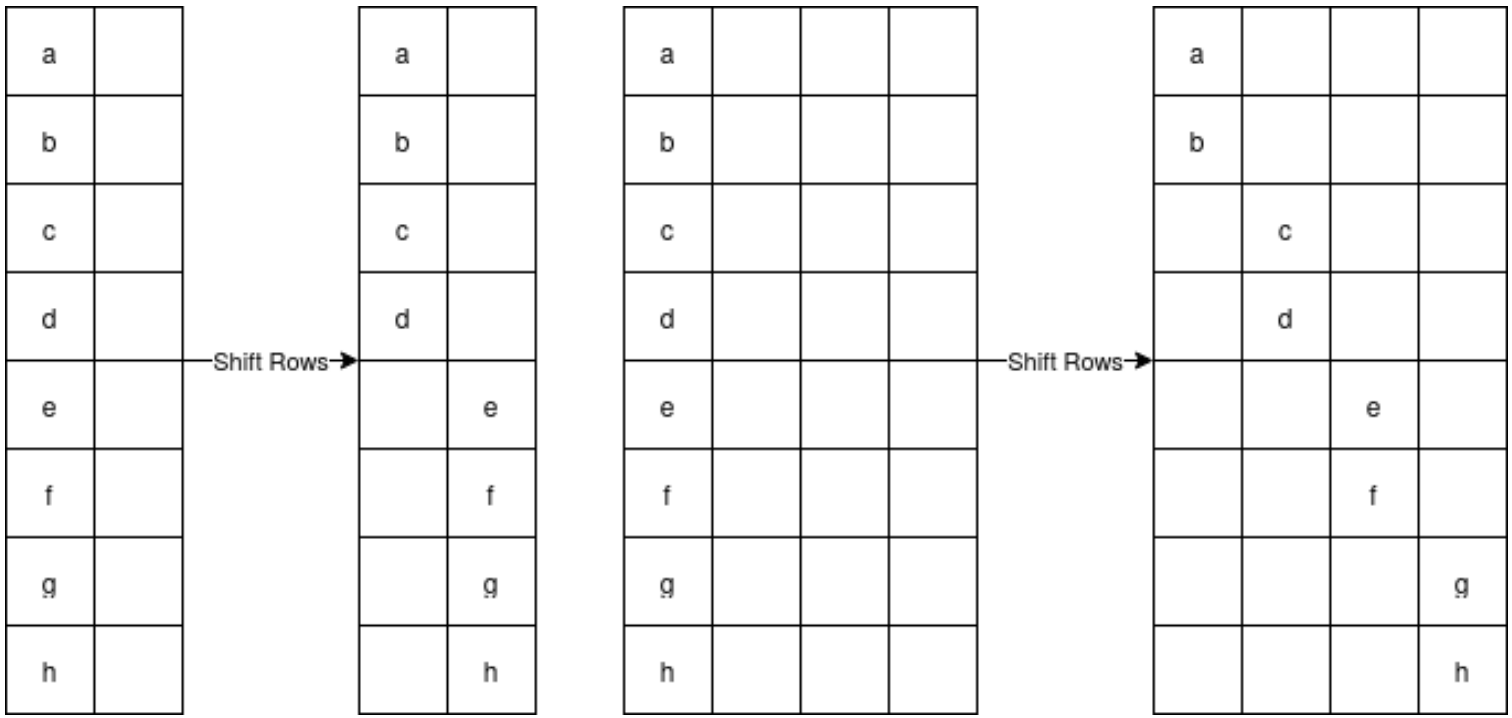


Outline

Applying Confusion: Sub Bytes

- Confusion to obscure the relationship of each byte.
- Each byte into a substitution box(S-Box), which map it to a different byte.
- There are 4 different S-Boxes. $\forall$ cell of state $g_{i,j}$, Kalyna uses $S_{i\%4}$ S-box for substitution.

Applying Diffusion: Shift Row



- Cyclic right shift for the rows of the state matrix.
- shift $= \lfloor \frac{i.l}{512} \rfloor$, i row no, $l \in 128, 256, 512$ is block size

Mix Columns

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 01.a_0 \oplus 01.a_1 \oplus 05.a_2 \oplus 01.a_3 \oplus 08.a_4 \oplus 06.a_5 \oplus 07.a_6 \oplus 04.a_7 \\ 04.a_0 \oplus 01.a_1 \oplus 01.a_2 \oplus 05.a_3 \oplus 01.a_4 \oplus 08.a_5 \oplus 06.a_6 \oplus 07.a_7 \\ 07.a_0 \oplus 04.a_1 \oplus 01.a_2 \oplus 01.a_3 \oplus 05.a_4 \oplus 01.a_5 \oplus 08.a_6 \oplus 06.a_7 \\ 06.a_0 \oplus 07.a_1 \oplus 04.a_2 \oplus 01.a_3 \oplus 01.a_4 \oplus 05.a_5 \oplus 01.a_6 \oplus 08.a_7 \\ 08.a_0 \oplus 06.a_1 \oplus 07.a_2 \oplus 04.a_3 \oplus 01.a_4 \oplus 01.a_5 \oplus 05.a_6 \oplus 01.a_7 \\ 01.a_0 \oplus 08.a_1 \oplus 06.a_2 \oplus 07.a_3 \oplus 04.a_4 \oplus 01.a_5 \oplus 01.a_6 \oplus 05.a_7 \\ 05.a_0 \oplus 01.a_1 \oplus 08.a_2 \oplus 06.a_3 \oplus 07.a_4 \oplus 04.a_5 \oplus 01.a_6 \oplus 01.a_7 \\ 01.a_0 \oplus 05.a_1 \oplus 01.a_2 \oplus 08.a_3 \oplus 06.a_4 \oplus 07.a_5 \oplus 04.a_6 \oplus 01.a_7 \end{bmatrix}$$

- Irreducible Polynomial $x^8 + x^4 + x^3 + x^2 + 1$.
- $M = (0x01, 0x01, 0x05, 0x01, 0x08, 0x06, 0x07, 0x04)$ is the vector that forms the circulant matrix with the MDS property.

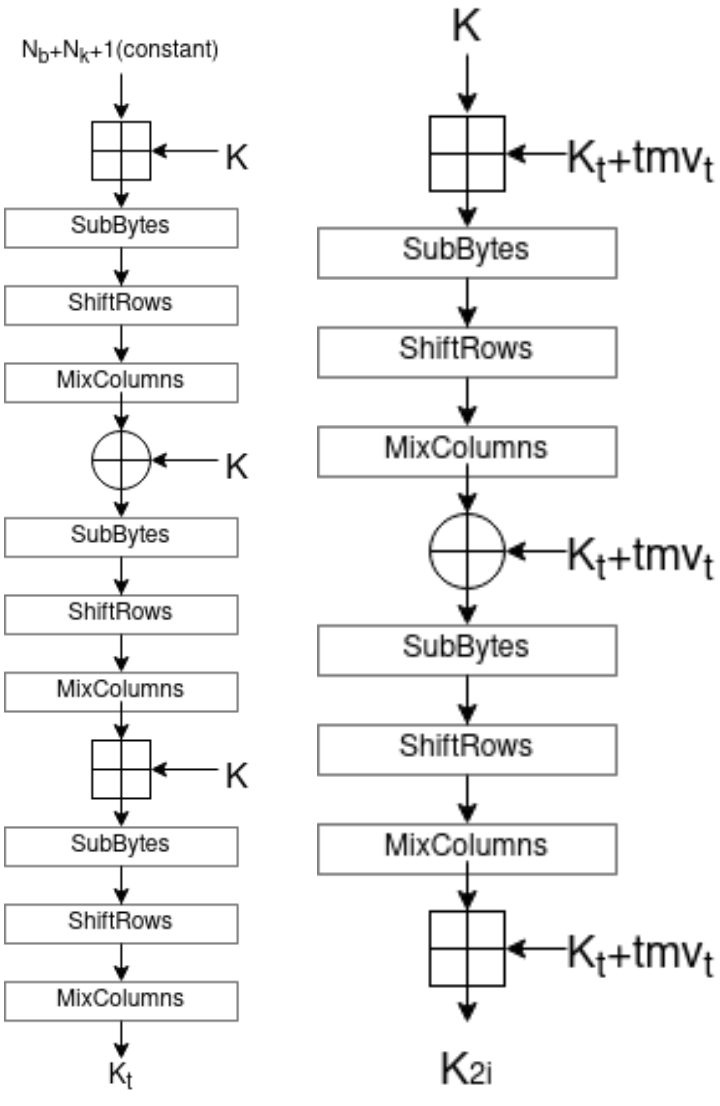
Addition modulo 2^{64}

- In mod 2^{64} addition select every column of the state is added to the every column of the round key.
- In the addition operation the little-endian convention is used, i.e. least significant byte at the lowest address.

Key Schedule: Round Key Generation

- Different for Even and Odd rounds
- Every $2i + 1^{th}$ round key is derived from $2i^{th}$ round key.

Key schedule overview



$$tmv_0 = \mu^{0x00010001...0001}$$

$$tmv_{i+2} = tmv_i << (i/2)$$

$$K = K >>> 32.i$$

$$K_i = (K_{i-1} <<< 2N_b + 3)$$

For odd round. N_b is the number of bytes in the state

Outline

DDT

DDT Info for S-Box 1	
Values	Number of values in the difference table
8	15
6	246
4	3423
2	24996
0	36345

- 56% of the difference table's values are "0", and 44 % are non-zero values for S-Box 1.
- Maximum value in the difference table for all S-Boxes is equal to 8.

Differential

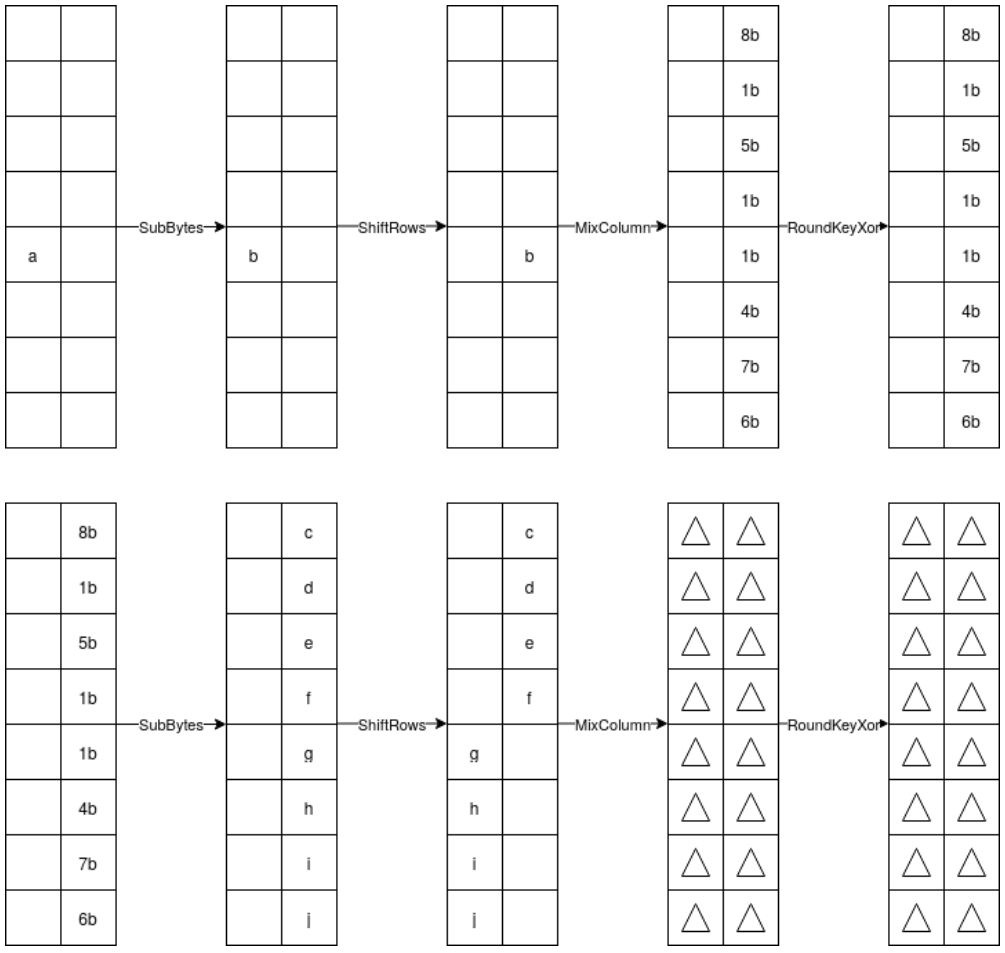


Figure: Difference propagation for two rounds of Kalyna

Integral

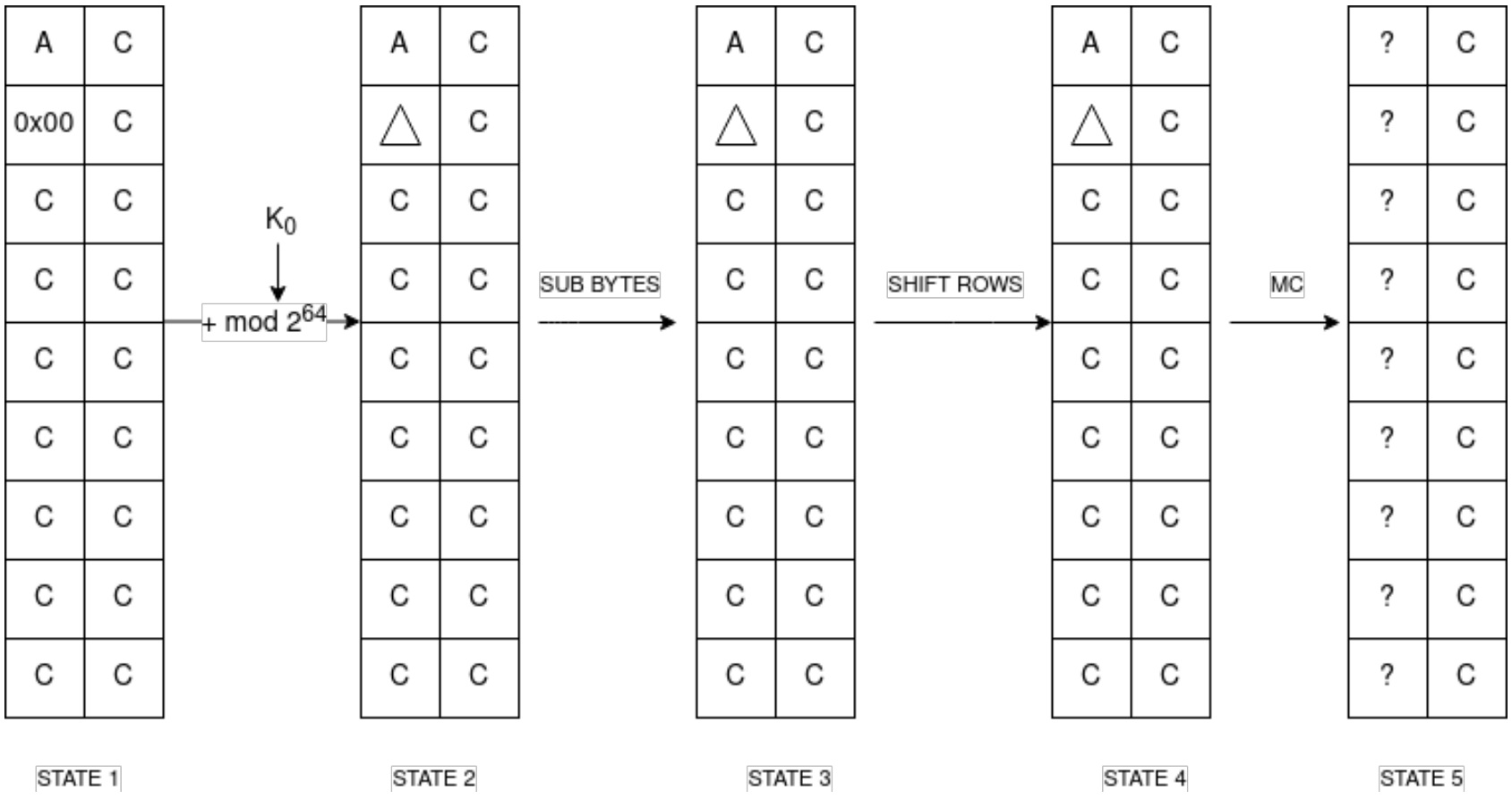


Figure: *All*, *Constant* property propagation

Integral Mix Column

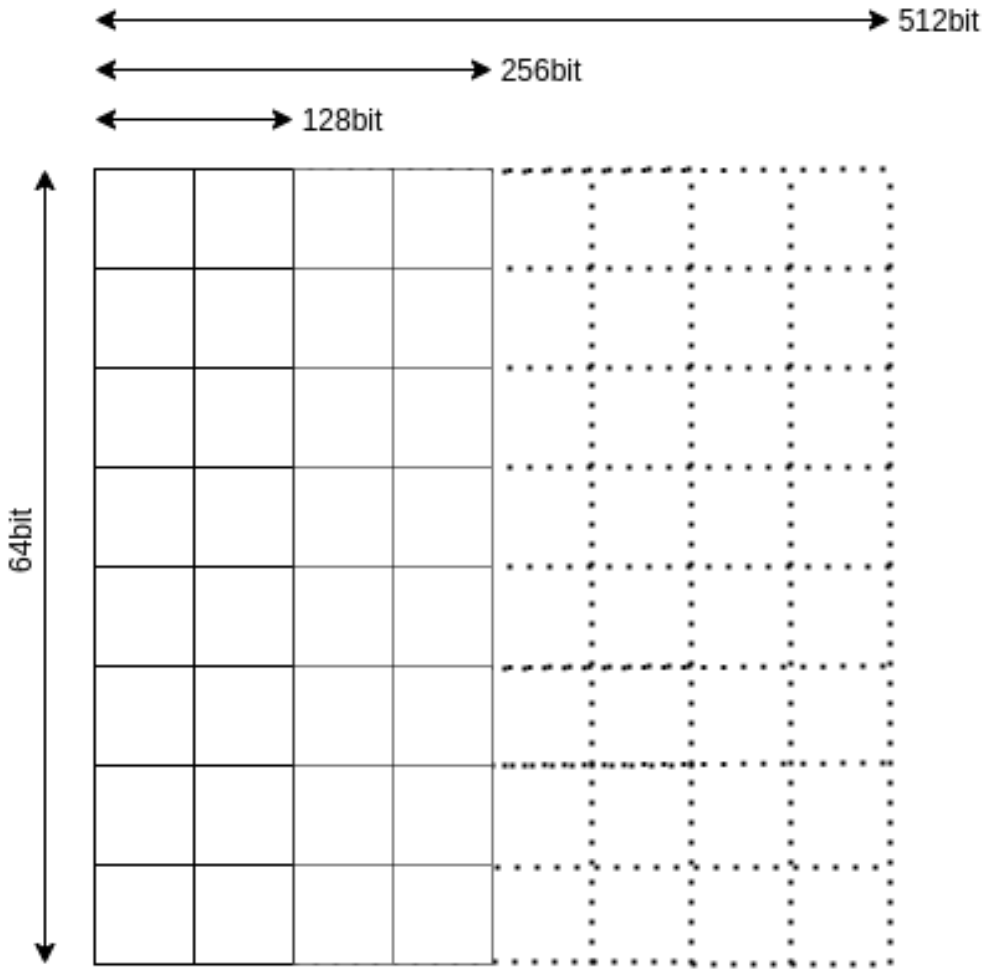
$$\begin{bmatrix} 1 & 1 & 5 & 1 & 8 & 6 & 7 & 4 \\ 4 & 1 & 1 & 5 & 1 & 8 & 6 & 7 \\ 7 & 4 & 1 & 1 & 5 & 1 & 8 & 6 \\ 6 & 7 & 4 & 1 & 1 & 5 & 1 & 8 \\ 8 & 6 & 7 & 4 & 1 & 1 & 5 & 1 \\ 1 & 8 & 6 & 7 & 4 & 1 & 1 & 5 \\ 5 & 1 & 8 & 6 & 7 & 4 & 1 & 1 \\ 1 & 5 & 1 & 8 & 6 & 7 & 4 & 1 \end{bmatrix} \times \begin{bmatrix} i \\ \Delta \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} = \begin{bmatrix} 1i \oplus 1\Delta \oplus 5c_2 \oplus 1c_3 \oplus 8c_4 \oplus 6c_5 \oplus 7c_6 \oplus 4c_7 \\ 4i \oplus 1\Delta \oplus 1c_2 \oplus 5c_3 \oplus 1c_4 \oplus 8c_5 \oplus 6c_6 \oplus 7c_7 \\ 7i \oplus 4\Delta \oplus 1c_2 \oplus 1c_3 \oplus 5c_4 \oplus 1c_5 \oplus 8c_6 \oplus 6c_7 \\ 6i \oplus 7\Delta \oplus 4c_2 \oplus 1c_3 \oplus 1c_4 \oplus 5c_5 \oplus 1c_6 \oplus 8c_7 \\ 8i \oplus 6\Delta \oplus 7c_2 \oplus 4c_3 \oplus 1c_4 \oplus 1c_5 \oplus 5c_6 \oplus 1c_7 \\ 1i \oplus 8\Delta \oplus 6c_2 \oplus 7c_3 \oplus 4c_4 \oplus 1c_5 \oplus 1c_6 \oplus 5c_7 \\ 5i \oplus 1\Delta \oplus 8c_2 \oplus 6c_3 \oplus 7c_4 \oplus 4c_5 \oplus 1c_6 \oplus 1c_7 \\ 1i \oplus 5\Delta \oplus 1c_2 \oplus 8c_3 \oplus 6c_4 \oplus 7c_5 \oplus 4c_6 \oplus 1c_7 \end{bmatrix}$$

$$= \begin{bmatrix} 1i \\ 4i \\ 7i \\ 6i \\ 8i \\ 1i \\ 5i \\ 1i \end{bmatrix} \oplus \begin{bmatrix} 1\Delta \oplus 5c_2 \oplus 1c_3 \oplus 8c_4 \oplus 6c_5 \oplus 7c_6 \oplus 4c_7 \\ 1\Delta \oplus 1c_2 \oplus 5c_3 \oplus 1c_4 \oplus 8c_5 \oplus 6c_6 \oplus 7c_7 \\ 4\Delta \oplus 1c_2 \oplus 1c_3 \oplus 5c_4 \oplus 1c_5 \oplus 8c_6 \oplus 6c_7 \\ 7\Delta \oplus 4c_2 \oplus 1c_3 \oplus 1c_4 \oplus 5c_5 \oplus 1c_6 \oplus 8c_7 \\ 6\Delta \oplus 7c_2 \oplus 4c_3 \oplus 1c_4 \oplus 1c_5 \oplus 5c_6 \oplus 1c_7 \\ 8\Delta \oplus 6c_2 \oplus 7c_3 \oplus 4c_4 \oplus 1c_5 \oplus 1c_6 \oplus 5c_7 \\ 1\Delta \oplus 8c_2 \oplus 6c_3 \oplus 7c_4 \oplus 4c_5 \oplus 1c_6 \oplus 1c_7 \\ 5\Delta \oplus 1c_2 \oplus 8c_3 \oplus 6c_4 \oplus 7c_5 \oplus 4c_6 \oplus 1c_7 \end{bmatrix}$$

Outline

Brownie Point

We nominate this figure for brownie point.



This figure is same as we made for "About state" slide.

Why Chosen this?

- We have difficulty at start to understand the state
- This will definately help for new reader
- State Matrix visual is not avilable for Kalyna

Outline

Conclusion

- Differential and Integral Cryptanalysis
- DC is not same as AES
- IC cannot be done same as AES
- Further improvement on integral attack can be done

Thanks

Team Members

- Himanshu Sekhar Nayak
- Shivam Sharma
- Ayush Gupta

Implementation Info

- Github Link: