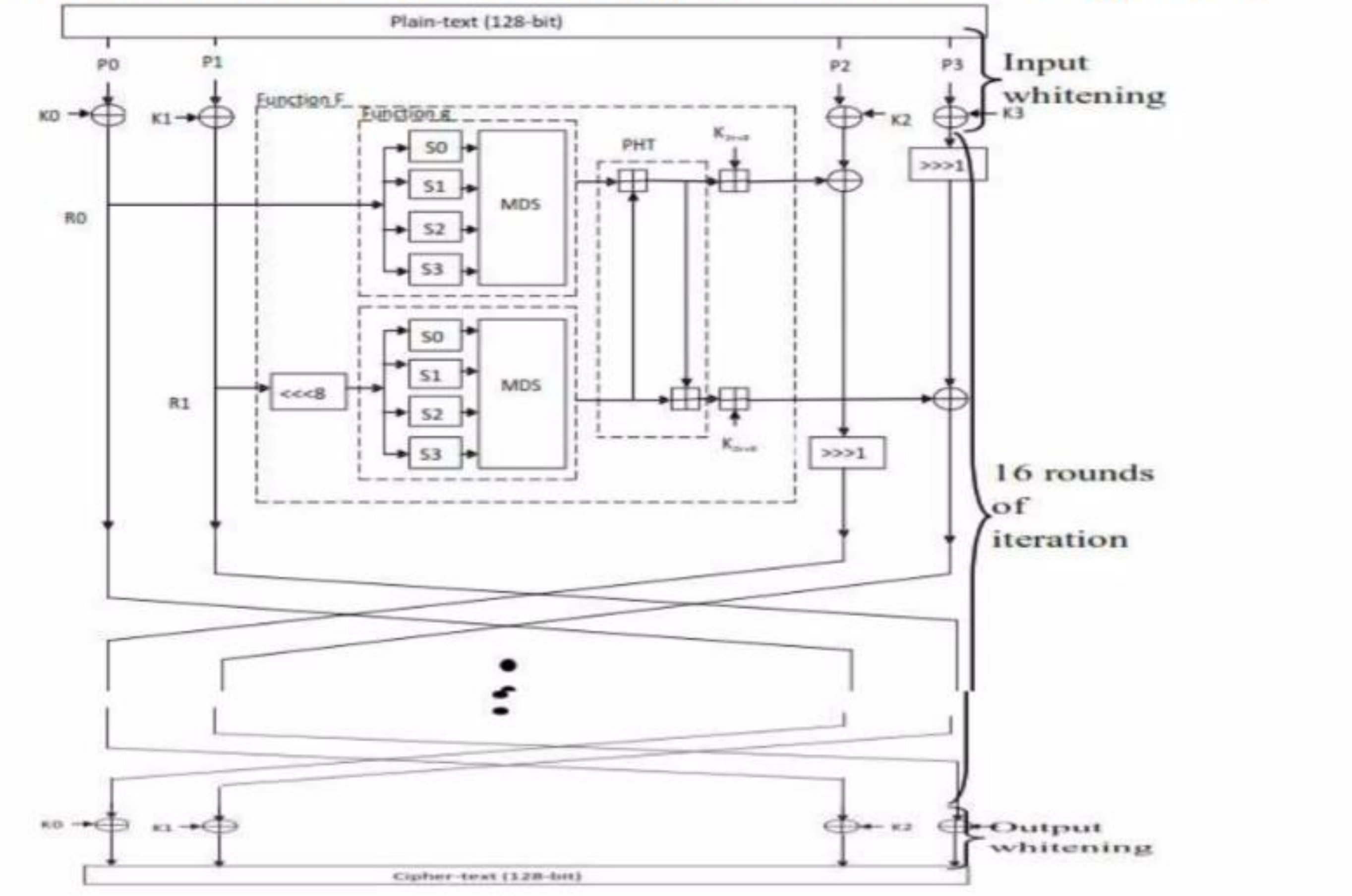
Twofish
A Block Encryption Algorithm

Presented by Nazar Yuras

Overview

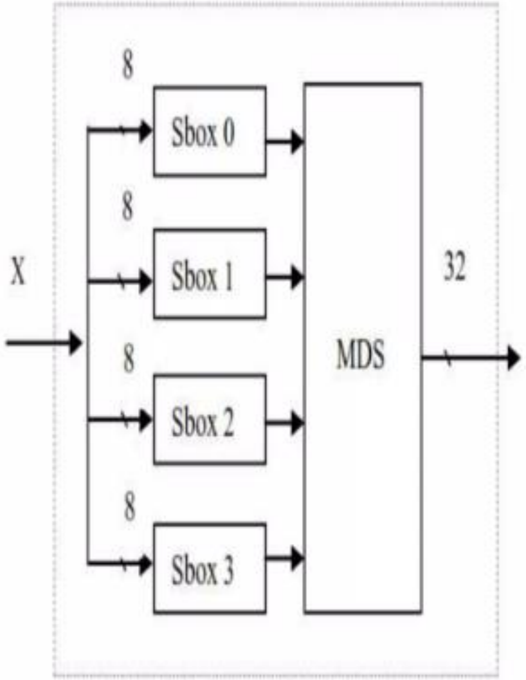
- Twofish is a symmetric key block cipher with a block size of 128 bits .
- It was first published in 1998.
- It was designed by Bruce Schneier.
- Twofish derived from Blowfish and Square.
- Twofish uses 16-rounds.
- key size of this cipher is 128 bits or 192 bits or 256 bits.

Twofish Round Function Block Diagram



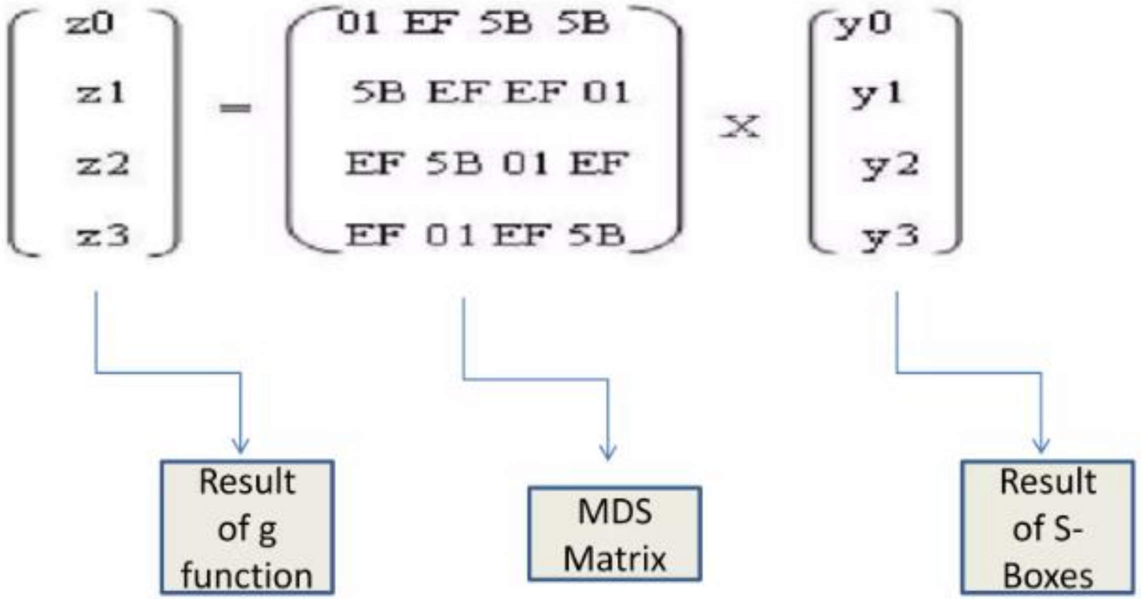
G-Function

- The function g forms the heart of Twofish.
- The input word X is split into four bytes. Each byte is run through its own key dependent S-box.
- Each S-box takes 8 bits of input, and produces 8 bits of output.
- The four results are interpreted as a vector of length 4 and multiplied by the 4X4 MDS (maximum distance separable) matrix.



G-Function (Cont:)

- The resulting vector is interpreted as a 32-bit word which is the result of g.



$$\begin{pmatrix} z0 \\ z1 \\ z2 \\ z3 \end{pmatrix} = \begin{pmatrix} 01 & EF & 5B & 5B \\ 5B & EF & EF & 01 \\ EF & 5B & 01 & EF \\ EF & 01 & EF & 5B \end{pmatrix} \times \begin{pmatrix} y0 \\ y1 \\ y2 \\ y3 \end{pmatrix}$$

PHT

- PHT is a reversible transformation of a bit string that provides cryptographic diffusion.

- Twofish uses a 32-bit PHT to mix the outputs from its two parallel 32-bit g functions.

- PHT have given two inputs, a and b.

Twofish Algorithm

- The plaintext is split into four 32-bit words.
- In the first step of input , these are x-ored with four key words as shown in the diagram.
- In each round, the two words on the left are used as input to the g functions. (One of them is rotated by 8 bits first.)

Twofish Algorithm (Cont:)

- The g function consists of four byte-wide key-dependent S-boxes, followed by a linear mixing step based on an maximum distance separable (MDS) matrix.
- The results of the two g functions are combined using a Pseudo-Hadamard Transform (PHT), and two keywords are added.

Twofish Algorithm (Cont:)

- These two results are then x-ored into the words on the right (one of which is rotated left by 1 bit first, the other is rotated right afterwards).
- The left and right halves are then swapped for the next round.

Cipher Text

- The undoes the `swap' of the last round.
- The four words of cipher text are then written as 16 bytes c0 ……….. c15 .
- The decryption procedure of Twofish can be done in the same way as the encryption procedure by reversing the order of the sub-keys,

THANK YOU