Aviv Abramovich

Diagonal Order Matrix Transpose

Square Diagonal Matrices Formula:

let A be squares diagonal order matrix, plain text or encrypted, so A is vector of vectors, that each of these sub-vectors are a diagonal in A: . Let B_i be the i-th diagonal vector in the transposed matrix, so we can calculate it that way

$$B_i = A_{-i \bmod n} <<< i$$

when $vec <<< j$ stands for “rotate the vector vec j indexes left (or -j to right).
Example:
I’ll prove that method works for 3*3 matrix, but it stands for any size of matrix.
Let A and B be 2 3*3 matrices:

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

So our result should be

$$B = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix}$$

if we disassemble A to diagonal vectors, it would be:
$A_0 = [a,e,i], A_1 = [b,f,g], A_2 = [c,d,h]$

and b should be :
$B_0 = [a,e,i], B_1 = [d,h,c], B_2 = [g,b,f]$

So if we use the formula for calculate C_0 we get:

$$B_0 = A_{-0 \bmod 3} <<< 0 = A_0 = [a,e,i]$$
$$B_1 = A_{-1 \bmod 3} <<< 1 = A_2 <<< 1 = [c,d,h] <<< 1 = [d,h,c]$$
$$B_2 = A_{-2 \bmod 3} <<< 2 = A_1 <<< 2 = [b,f,g] <<< 2 = [g,b,f]$$