diagonal round

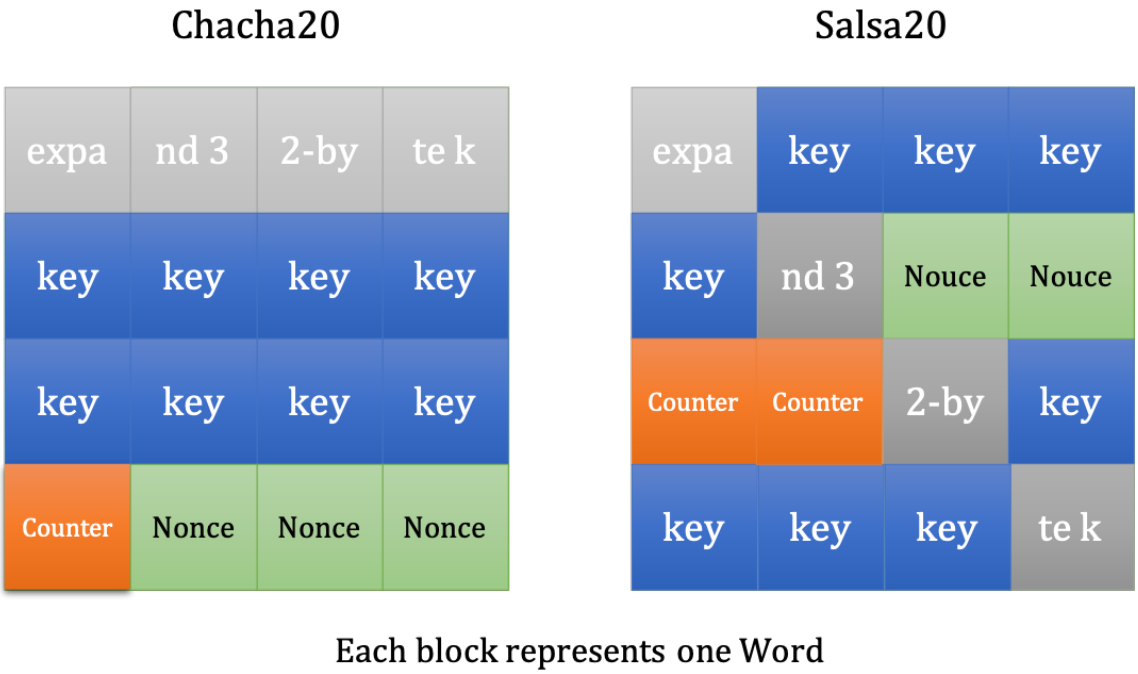
```
# chacha diagonal round
z[0], z[5], z[10], z[15] = qround_chacha([y[0], y[5], y[10], y[15]])
z[1], z[6], z[11], z[12] = qround_chacha([y[1], y[6], y[11], y[12]])
z[2], z[7], z[8], z[13] = qround_chacha([y[2], y[7], y[8], y[13]])
z[3], z[4], z[9], z[14] = qround_chacha([y[3], y[4], y[9], y[14]])

# salsa20 row round
z[0], z[1], z[2], z[3] = qround_salsa(y[0:4])
z[5], z[6], z[7], z[4] = qround_salsa(y[5:8], y[4:5])
z[10], z[11], z[8], z[9] = qround_salsa(y[10:12], y[8:10])
z[15], z[12], z[13], z[14] = qround_salsa(y[15:16], y[12:15])
```

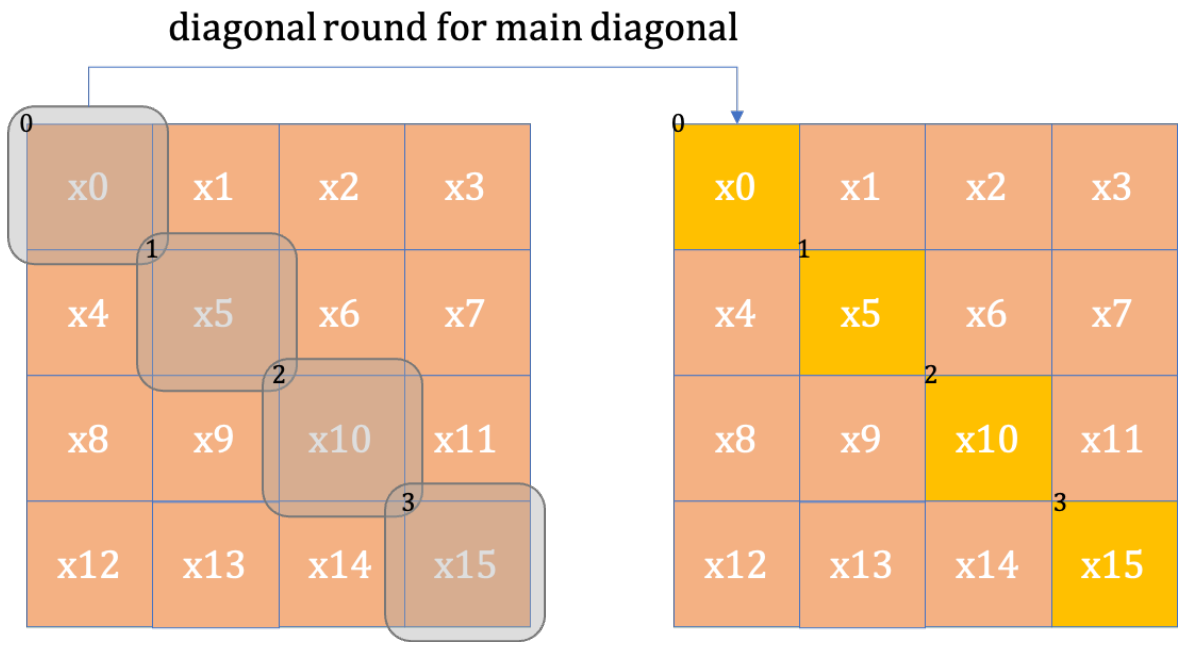
The diagonal round function in ChaCha is similar to the "row round" function but there are still something different.

Firstly, one thing that must be shown is that the initial state of chacha is different from the one in Salsa20.

In Salsa20, the initial state matrix is composed unorderly while the Chacha matrix puts all the stuff in order. As shown in the Fig1, the gray block represents the constant, the blue block represents the key, the orange block represents the counter of message and the green block represents nonce which can be used only once.



After knowing that, the diagonal round function has a similar effect to row round which shuffle the rows of matrix. However, the diagonal transformation has both vertical and horizontal effects. Specifically, the function firstly invertibly transforms the main diagonal using the quarter-round which has been explained before. Then, apply the same function to lists (i.e. [1,6,11,12], [2,7,8,13] and [3,4,9,14]).

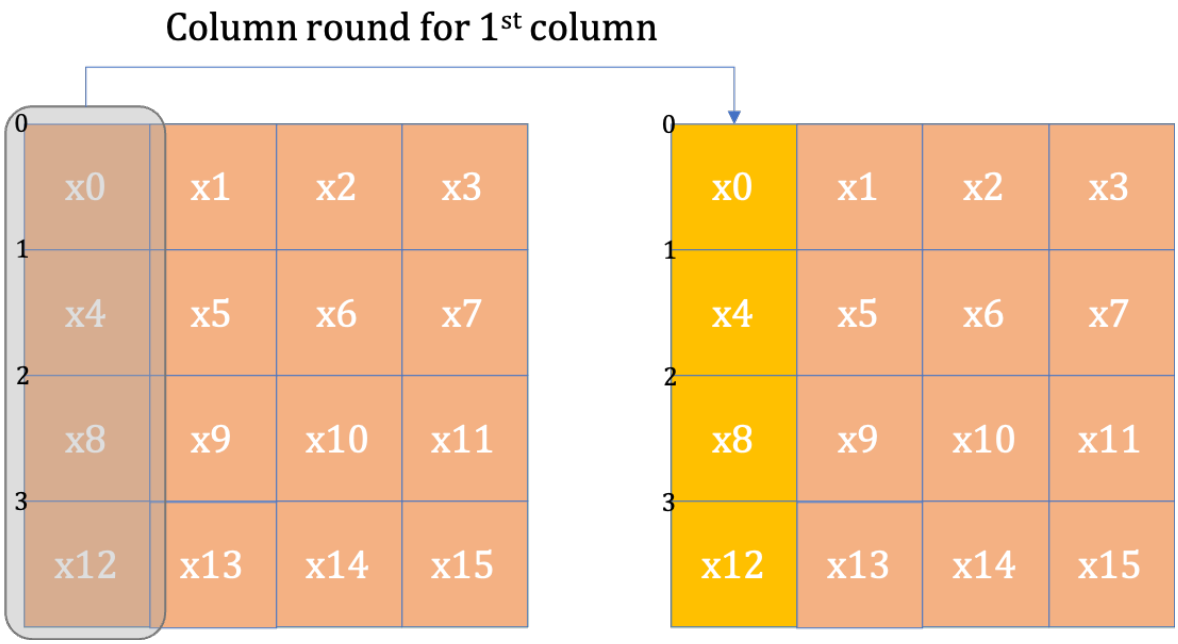


column round

```
# salsa20
y[ 0], y[ 4], y[ 8], y[12] = qround_salsa([x[ 0], x[ 4], x[ 8], x[12]])
y[ 5], y[ 9], y[13], y[ 1] = qround_salsa([x[ 5], x[ 9], x[13], x[ 1]])
y[10], y[14], y[ 2], y[ 6] = qround_salsa([x[10], x[14], x[ 2], x[ 6]])
y[15], y[ 3], y[ 7], y[11] = qround_salsa([x[15], x[ 3], x[ 7], x[11]])

# chacha20
y[0], y[4], y[8], y[12] = qround_chacha([x[0], x[4], x[8], x[12]])
y[1], y[5], y[9], y[13] = qround_chacha([x[1], x[5], x[9], x[13]])
y[2], y[6], y[10], y[14] = qround_chacha([x[2], x[6], x[10], x[14]])
y[3], y[7], y[11], y[15] = qround_chacha([x[3], x[7], x[11], x[15]])
```

The "column round" function of chacha20 has the same effect of column round of salsa20, which shuffle the rows in initial and intermediate state matrix. Specifically, the round function applies each row respectively.



As shown in the previous code segment, column round in chacha feed the function in order while the one in salsa20 does not.

I speculate that shuffling the order is not beneficial for security and also handling the input in order can be speeded up in some machines. Therefore, the order shuffling was canceled for no good reasons.

double round

```
# chacha
diagonalround(columnround(x))
# salsa20
rowround(columnround(x))
```

For the double round function, which is composed of two round functions (i.e. column round and diagonal round), just determine the order of the two functions "column round" and "diagonal round" which is as same as the one in salsa20.