Toy cipher —

It is an ARX cipher.

It takes two inputs each of size 4-bit and generates a 8-bit output.

The initial state $X^0 = x[1] \,||\, x[0]$.

or easily, $X^0 = \begin{pmatrix} x(1) & x(0) \end{pmatrix}_{1\times 2}$

This state goes through the following round:

Round-fun^n (a, b):

$$a' = a + b$$
$$a'' = (a' <<< 3)$$
$$a''' = a' \oplus a''$$
$$b''' = b + a'''$$

Generally $x(1)$ is the key and $x(0)$ is the plaintext.

Number of rounds = 5