Circom 101

BE bits $10011101 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + \ldots + 1 \cdot 2^7$
 $2^7\ 2^6 2^5\ 2^4 2^3\ 2^2\ 2^1\ 2^0$

LE bits $10111\ 001$
 $2^0\ 2^1\ 2^2 2^3\ 2^4\ 2^5\ 2^6\ 2^7$

Same for bytes, but bits inside bytes could be in different order.

BE bits := $\underset{2^N}{\longleftarrow}\overset{}{}\underset{2^0}{}$ arrow goes from less significant

LE bits := $\underset{2^0}{\longmapsto}\underset{2^N}{}$

BE bytes with BE bits := $\left[\longleftarrow \right]$
$ \longleftarrow$

Key Hash

key: $\longleftarrow$ $\left(\text{obtained from } \left[\longleftarrow \right]\right)$
$ \longleftarrow$

divide 128-bit key into bytes:

$$[\longleftarrow] \ [\longleftarrow] \ \ldots \ [\longleftarrow]$$
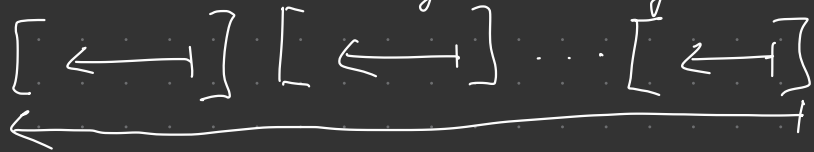
convert key bytes to little-entian:

$$[\longmapsto] \ [\longmapsto] \ \ldots \ [\longmapsto]$$

convert key to number:

$$[\longmapsto \ \longmapsto \ \ldots \ \longmapsto \ 0\,0\ldots0] \quad (254 \text{ bits})$$

component Bits2Num_strict

MiMC7 of the key number:

key number ⟶
key hash = 0 ⟶ MultiMiMC7 ⟶ key hash number
            1 input
            91 rounds

$\lfloor LEBits2BEBytes \rfloor$

$$[\longmapsto\longmapsto\longrightarrow] \quad to \quad [\longleftarrow\dashv][\longleftarrow\dashv]\cdots[\longleftarrow\dashv]$$

$$\cdots \quad to \quad \begin{bmatrix} byte \\ num & byte \\ num & \cdots & byte \\ num \end{bmatrix}$$