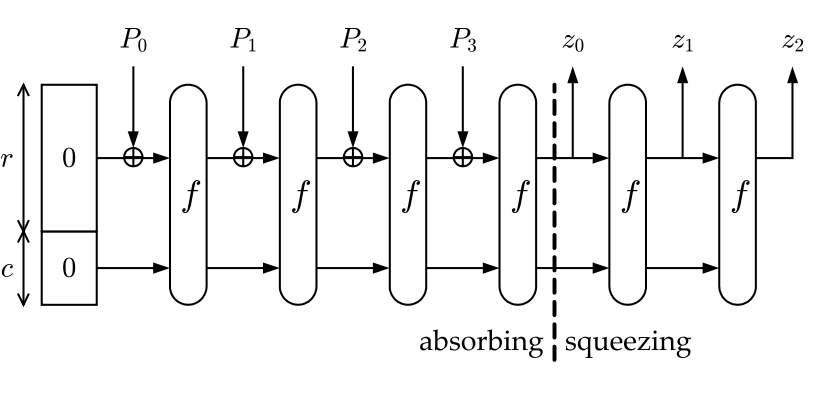
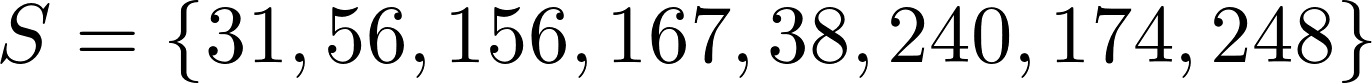
CictroHash

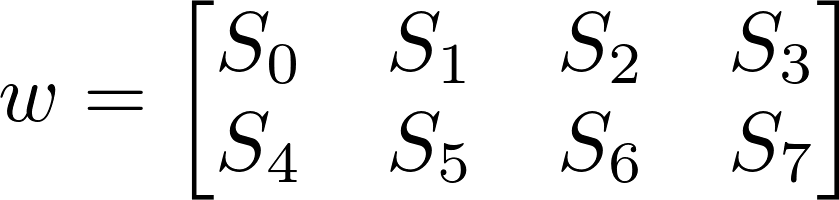
This document will describe the Hash Function CictroHash. It follows modern hashing techniques in a truly elegant and hardware-capable design. The sponge construction is a popular method used by hash functions to transfer through entropy to variable input. It is used in the ever-popular Keccak Hash function and is demonstrated below



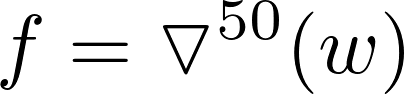
Note that for CictroHash the digest will simply be the value *z0*. Also, for CictroHash r is 4 bytes in length and c is four bytes in length. The starting state of r and c (denoted S) is shown below.



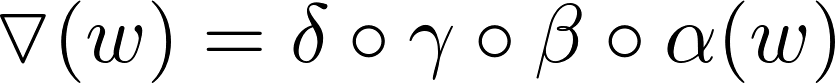
The pre-image for CictroHash is also padded to the nearest 4-byte increment by all zeros. The state transformation function *f* is a masterpiece in modern cryptography. It utilizes all of people’s favorite operations like left shift, right shift, left rotate, right rotate, and swapping! The first step of *f* is to take the state array S and put it into the matrix form like below (each element is a byte)



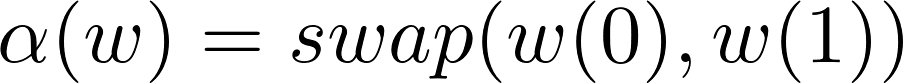
Then the round function () will be applied 50 times on *w*, or equivalently

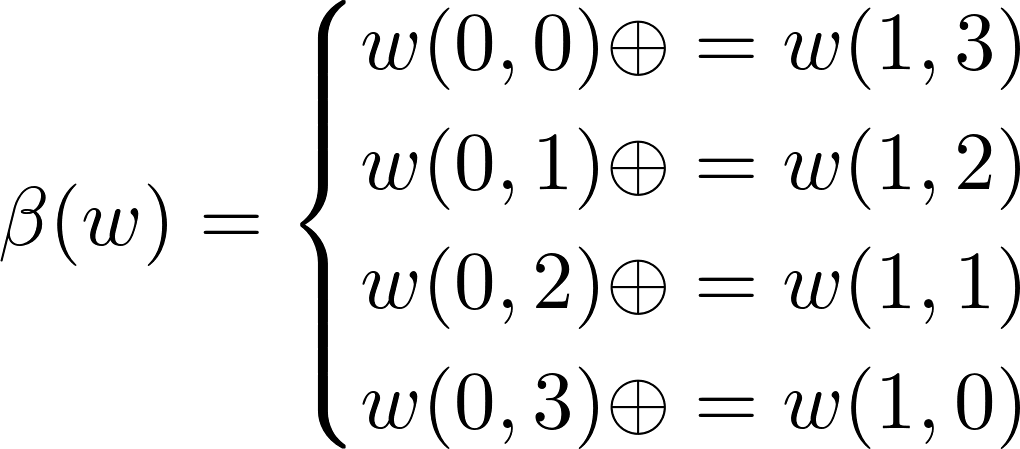


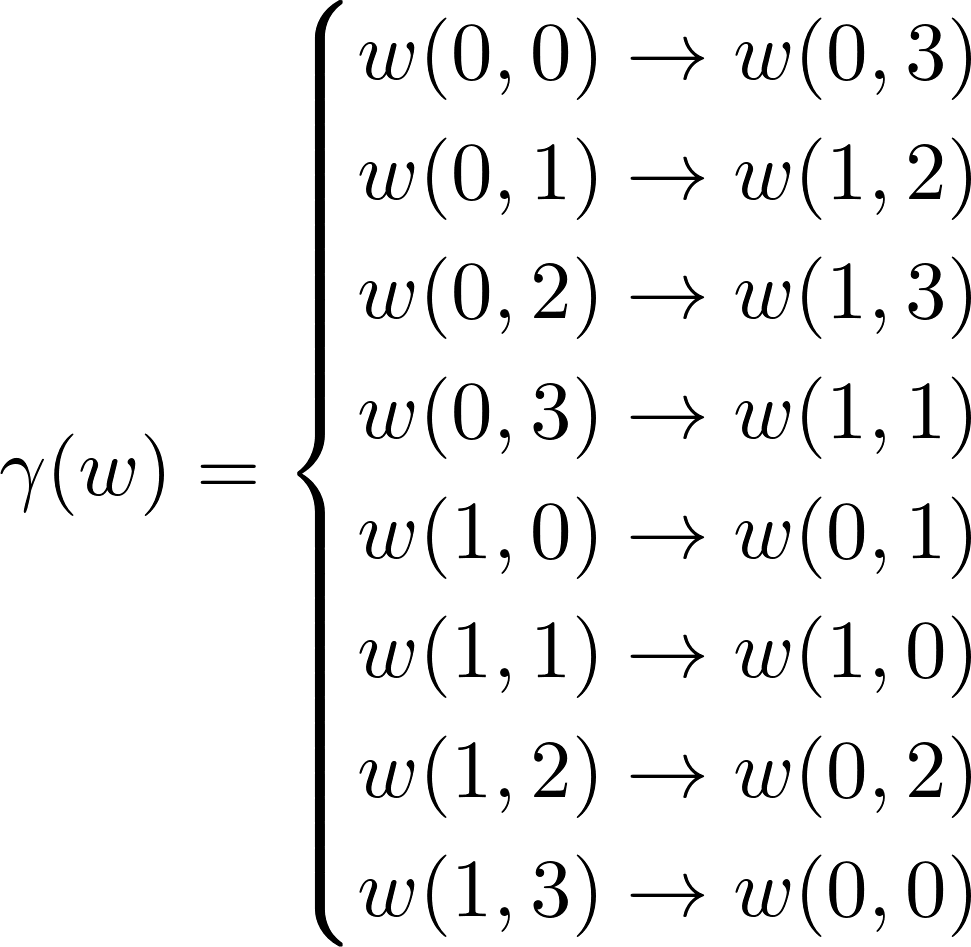
Finally, we can define as below

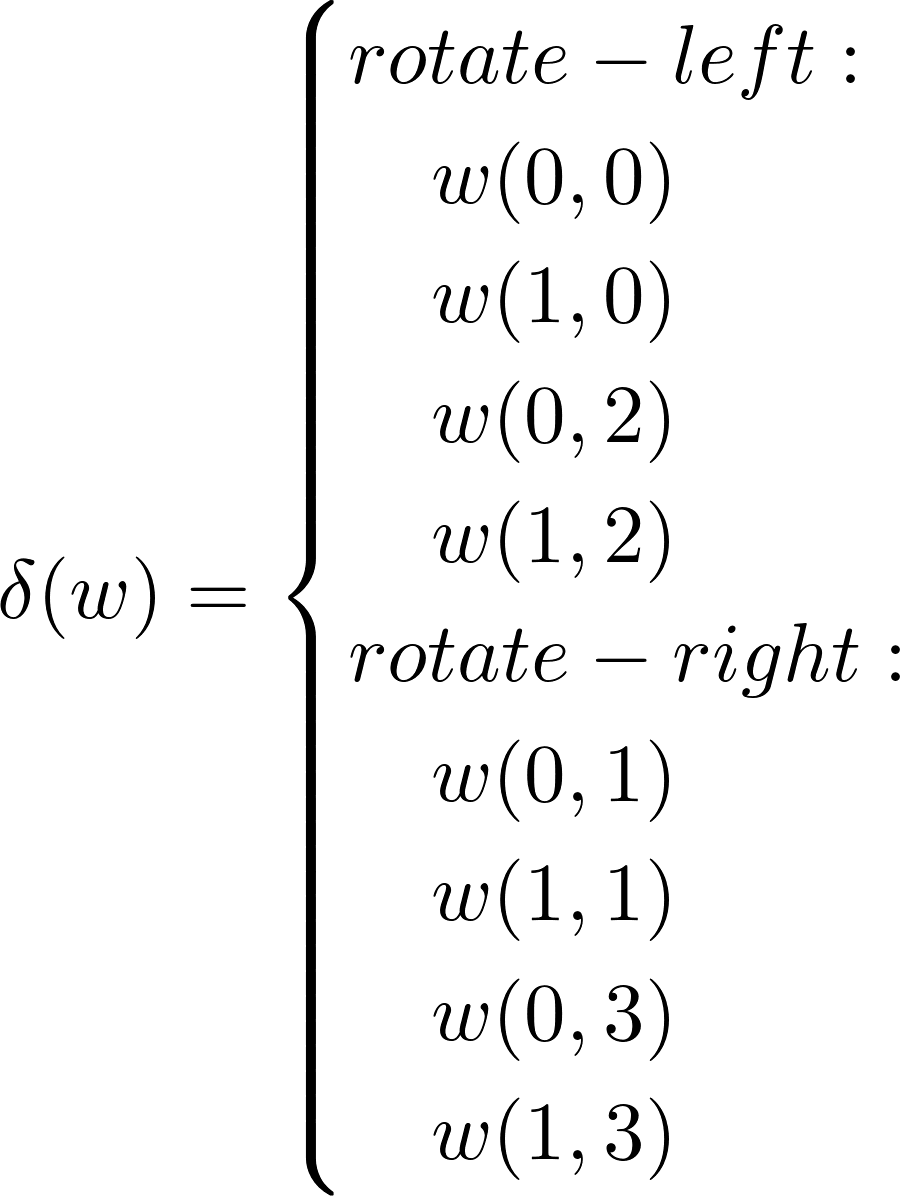


Clearly as is merely a composition of our trivial transformation we just need to define them, and we are done.









For the component the rotations will be 1-bit. After *z0* is calculated the last 4 bytes are dropped off to produce a 4-byte digest.

# Example Inputs/Outputs

CictroHash(HELLOWORLD) = 0xb5a79bee

CictroHash(GOODBYEWORLD) = 0xbc08f3d9

CictroHash(kUgKZMdQkn) = 0x38da3d00