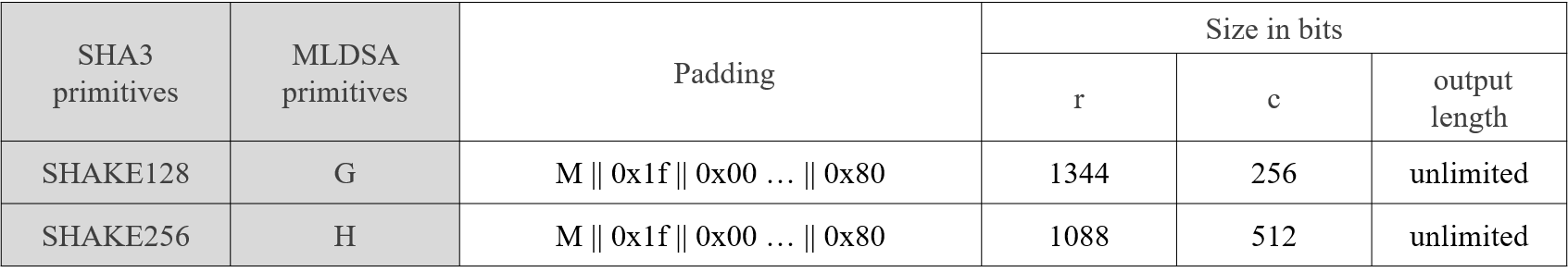
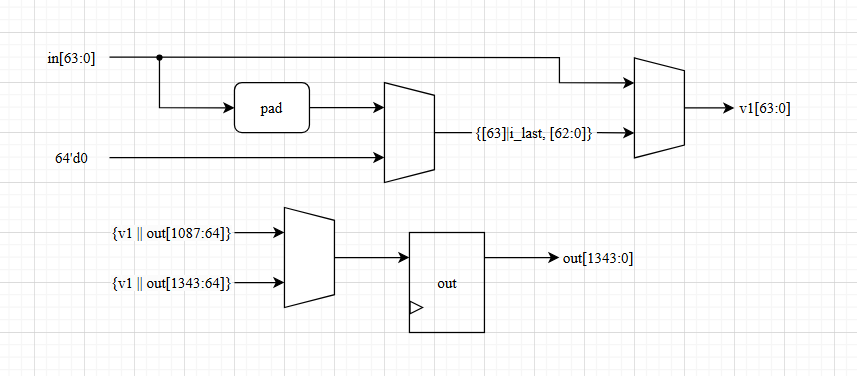
Keccak

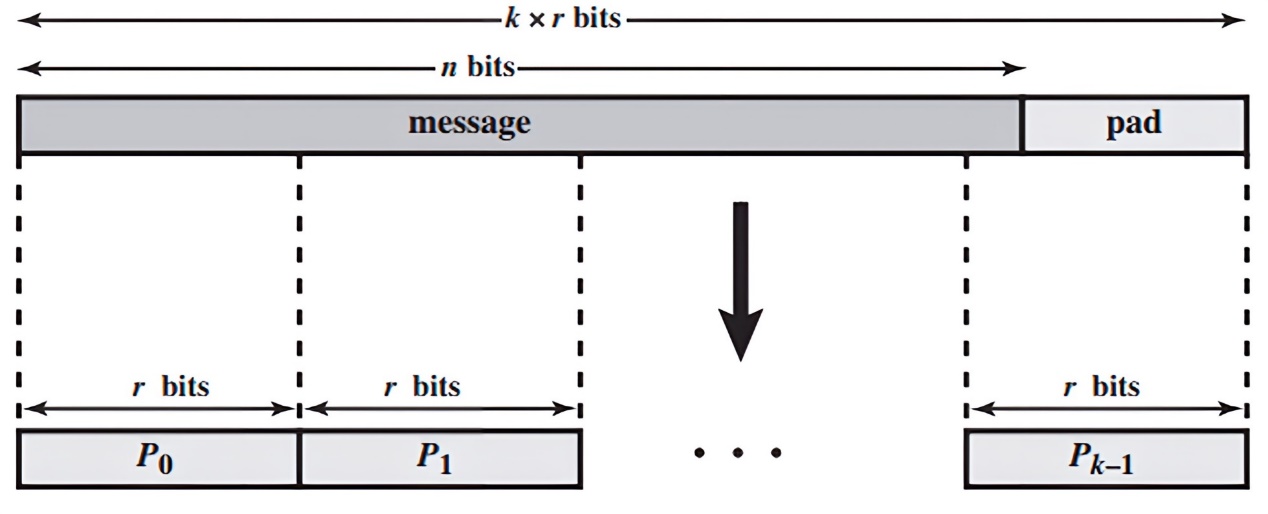
輸入為64bit，模式有G跟H兩種，分別為shake128與shake256，在sha3電路設計上我分為兩個主要的module，一個是Padder，專門處理資料輸入進來、shake需額外padding的4’d1111以及進行Multi-rate padding的部分，另外一個是F\_Permutation，專門處理Sponge Construction的部分。



1. Padder

每次輸入近來的資料長度為64bit，要padding一筆資料會分為3種情況，第一種就是一般的資料輸入，直接將輸入的64bit送進輸出的位移暫存器，而第二種是該筆64bit資料為剛好為1088或者1344的最後一個64bit輸入，則會將輸入送入pad當中並且將他的最後一位拉至1，最後一個情況是輸入的有效資料已經送完，但是還須補64’d0至1088或者1344，如果補的64’d0是最後一筆則將他的最後一位拉至1。當組合好1088或1344時，則會送出out\_ready信號告訴F\_Permutation可以動作。如果F\_Permutation正在運算且1344bit的暫存器被存滿則會透過buffer\_full告訴外界無法接收資料。





1. F\_Permutation

當Padder完成後，會透過in\_ready告訴F\_Permutation可以開始執行round function，最一開始進來會根據模式不同與out暫存器中的資料做xor，接者開始進行24round的round function，因為一次的round function是很長的組合電路，會成為整體電路的critical path，因此我根據路經delay長度將每次round functoin拆為兩段，第一次做theta、rho、pi，第二次做chi、iota，完成後會向Keccak送出out\_ready信號，如果輸出的有效資料不夠用，則可透過squeeze信號，讓F\_Permutation再產生有效資料。

