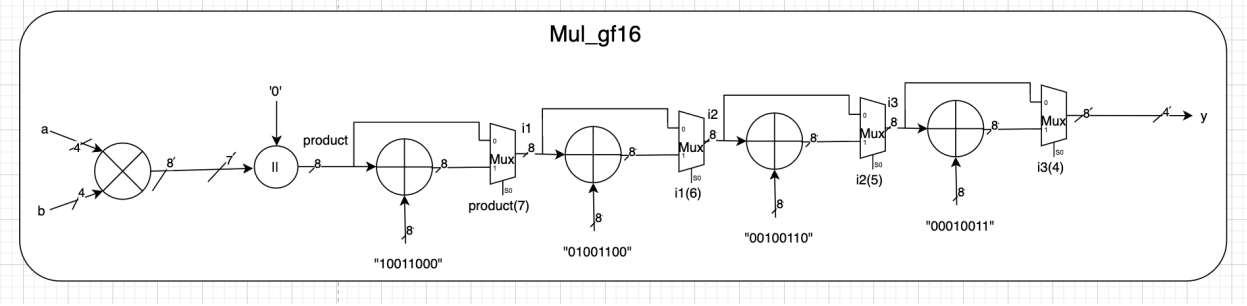
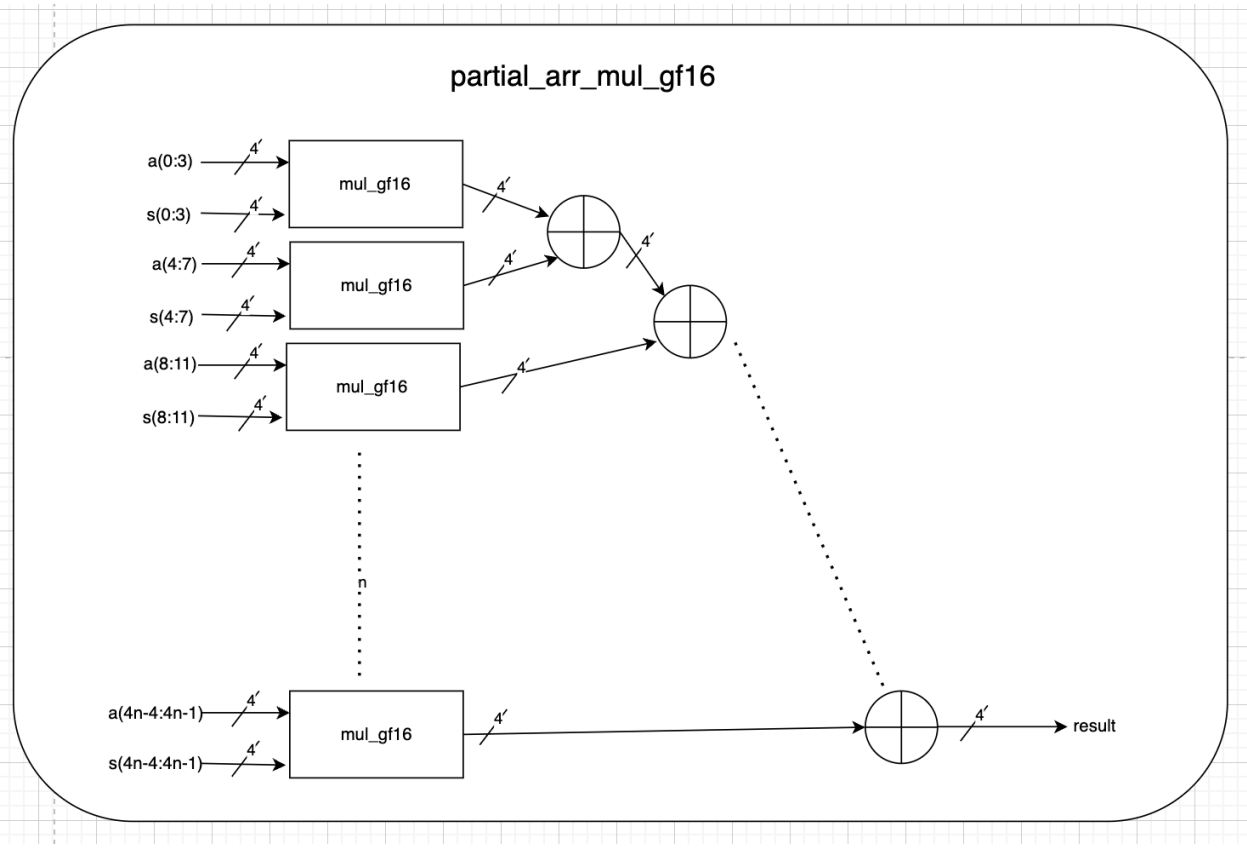
Detailed Block Diagrams

This module is used to multiply a,b with modulo reduction of x^4+x+1 to get 4 bit output y



This module is used to multiply all the elements in a row of array to a column of another array and XOR them to get a 4 bit output result



This module is used to reduce *z*4m* bit value using function f(z) = $z^{64}+x^3z^3+xz^2+x^3$ *to get 4m bit output y*