



GF(2<sup>8</sup>) Multiplier Detail

$\times 02 = \text{xtime}(x)$

left shift + cond. XOR 0x1B