

**128 bit
message**

127

0

**4 x 32-bit
chunks**

31 M3 0

31 M2 0

31 M1 0

31 M0 0