

SHA-256

$$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

$$Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z)$$

$$\Sigma_0(x) = RotR^2(x) \oplus RotR^{13}(x) \oplus RotR^{22}(x)$$

$$\Sigma_1(x) = RotR^6(x) \oplus RotR^{11}(x) \oplus RotR^{25}(x)$$

$$\sigma_0(x) = RotR^7(x) \oplus RotR^{18}(x) \oplus ShiftR^3(x)$$

$$\sigma_1(x) = RotR^{17}(x) \oplus RotR^{19}(x) \oplus ShiftR^{10}(x)$$

1 Words

$$W[i] = \begin{cases} 0 \leq i \leq 15 & M[i] \\ 16 \leq i \leq 63 & W[i] = \sigma_1(W[i-2]) + W[i-7] + \sigma_0(W[i-15]) + W[i-16] \end{cases}$$

2 Compression function

$$tmp_1 = h + \Sigma_1(e) + Ch(e, f, g) + K[i] + W[i]$$

$$tmp_2 = \Sigma_0(a) + Maj(a, b, c)$$

$$h = g$$

$$g = f$$

$$f = e$$

$$e = d + tmp_1$$

$$d = c$$

$$c = b$$

$$b = a$$

$$a = tmp_1 + tmp_2$$