000000000000000000000000000000

a b c d e f g h

+∑

**CH**AJ

**MAJ**AJ

**∑**∑

**∑**∑

**+**∑

Wt

**+**∑

**+**∑

**+**

Kt

**+**∑

**+**∑

512 bits

a b c d e f g h