state:

16 32-bit values

20 rounds

ARX ← xor

addition

rotation